Out-of-the-Lab Research in Usable Security and Privacy

Florian Alt
florian.alt@unibw.de
Bundeswehr University Munich
Munich, Bavaria, Germany

Figure 1: Approaches to out-of-the-lab research in usable security and privacy: Researchers can provide experiments in the form of apps or services – either as stand-alone apps (e.g. SmudgeSafe [18], left) or piggyback apps (e.g., the ResearchIME smartphone keyboard [4], middle) – or they can implement experiments in VR to enable participation from home [11], right).

ABSTRACT

The COVID pandemic made it challenging for usable security and privacy researchers around the globe to run experiments involving human subjects, specifically in cases where such experiments are conducted in controlled lab setting. Examples include but are not limited to (a) observing and collecting data on user behavior with the goal of (b) informing the design and (c) engineering novel concepts based on adaptation and personalization as well as (d) evaluating such concepts regarding user performance and robustness against different threat models. In this keynote I will set out with providing a brief introduction to and examples on our research on behavioral biometrics. I will then discuss how the current situation influences research requiring close work with human subjects in lab settings and outline approaches to address emerging issues. Finally, I will provide some examples of out-of-the-lab research and reflect on both challenges and opportunities of these approaches.

CCS CONCEPTS

• **Security and privacy → Security services**; • **Human-centered computing → HCI design and evaluation methods**.

KEYWORDS

usable security, evaluation methods, behavioral biometrics

UMAP '21 Adjunct, June 21–25, 2021, Utrecht, Netherlands

ACM ISBN 978-1-4503-8367-7/21/06.
https://doi.org/10.1145/3450614.3464468

ACM Reference Format:
Florian Alt. 2021. Out-of-the-Lab Research in Usable Security and Privacy. In *Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization (UMAP '21 Adjunct), June 21–25, 2021, Utrecht, Netherlands.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3450614.3464468

1 INTRODUCTION

Research in Usable Security and Privacy employs a wide range of research approaches – from observing and understanding user behavior in security-critical situations (for example, how they behave as they are exposed to a phishing email [12], how they chose secrets in knowledge-based authentication schemes [19, 22]) via designing and implementing novel security and privacy concepts (for example, a new authentication mechanism [3, 21], a training app to raise awareness for social engineering attacks [9, 20]) to evaluating such novel concepts (for example, how easily users can learn them [2], how well they protect against different user-centered attacks [1]). While much research in our community is conducted in the form of surveys and interviews, still a considerable part of our work is conducted in controlled lab settings, in particular when evaluating novel approaches and concepts with users.

The guiding example I will use in this keynote talk is research on behavioral biometrics, that is the use of behavioral patterns in human behavior to identify individuals. Much of the work in this area requires collecting data on user behavior (such as touch targeting [6] and typing on a smartphone [5] or also behavior while manipulating or interacting with objects in VR [13] with the objective of then training user models based on the collected data. Ultimately, these models can be used to identify users and use this information, for example, to build novel authentication mechanisms based on continuous authentication [7][1].

[1]Note, that many other use cases exist for behavioral biometrics, such as building adaptive user interfaces.

Such research has lately become challenging as a result of the COVID pandemic, which made it increasingly difficult to run experiments with human subjects in research labs. As a result, researchers were (and still are) forced to rethink their way of doing research, for example, obtaining data from other sources, thinking of ways to conduct research outside the lab, appropriating their research questions, or coming up with entirely new ways of doing research.

In this keynote talk I will provide an overview of alternative approaches to out-of-the-lab research (cf section 2). Afterwards I will provide examples from my own research and discuss challenges and opportunities researchers are facing as they apply these approaches to usable security and privacy research (cf. section 3).

2 OUT-OF-THE-LAB RESEARCH

The HCI community has early on recognized the need for rethinking common approaches to research. As a result, the past year witnessed several panel discussions[2], courses at conferences[3] [17], overviews of research approaches [16], and special issues[4].

The following section summarizes some of the approaches

Using Existing Stuff Rather than collecting new data sets, researchers could use existing data sets. Such data sets are often made available by other researchers upon request. An example is a data set by Khamis et al. with images taken from the front-facing camera of a smartphone to better understand users' behavior [10]. Similarly, researchers might discover new research questions they could answer based on their own data they had previously collected. Also, online forums or rating features (for example, for apps, products, services, hotels, etc.) may provide fertile ground for interesting research questions related to privacy and / or security.

Web and App Usage Prior research has already shown that technologies being available to many users (such as web browsers, smartphones, smart watches) can be used for research purposes. Several approaches exist: firstly, web services, such as Amazon MTurk [14] and Prolific, can be used for *crowd-sourcing* information. Secondly, *standalone applications* can be distributed through app stores for download by any user. An example is the SmudgeSafe app, an authentication app that Schneegass et al., made available through GooglePlay and that was downloaded by 1500 users [18]. Thirdly, research prototypes can be *piggybacked* with existing applications. For example, Buschek et al. built a custom keyboard for use on Android devices. In this way, they were able to collect keystroke dynamics as participants used different types of apps [4].

Users at Home Another approach is to think about how experiments can be conducted in users' homes. Whereas communication with users (for example, interviews) can be easily conducted using video conferencing tools, more sophisticated setups could entail the use of cameras and screencasts as participants solve web-based tasks on their PC. For example, Fröhlich et al., investigated user behavior while trying to purchase cryptocurrency [8]. Another approach is to supply study equipment to participants at home, for example, sending them an eye tracker to try out a new gaze-based authentication mechanism.

New Approaches Researchers can come up with entirely new approaches. For example, researchers might employ *analytic or computational* evaluation methods. Approaches such as GOMS or KLM (and its many variants) allow different systems to be compared (in particular, regarding the required number of basic operations). Another approach that recently received considerable attention is using VR as a complementary method to real-world research. Here, researchers can rebuilt real-world settings and observe users' behavior [15].

3 CHALLENGES AND OPPORTUNITIES

Out-of-the-lab research comes with a number of challenges.

Firstly, out-of-the-lab approaches are often characterized by less control over external influences, for example, participants might be interrupted, participate at different times of the day, etc. This influences the *validity* of the collected data. Specifically, the data is generally of lower internal validity but external and ecologic validity might be higher.

Second, an important criteria in research generally is *replicability*. To ensure replicability, researchers need to carefully think about how their study can be set up and all important aspects of the study be described in a way such that it is replicable.

Third, an opportunity of out-of-the-lab studies is investigating *long-term effects*. Whereas lab studies often just capture data at one specific moment in time, researchers could setup out-of-the-lab experiments to focus on how people behave, perform, or learn over a longer period of time. In usable security research this might be interesting when looking into the learnability of an approach or the memorability of secrets created with a novel scheme.

4 CONCLUSION

The ongoing pandemic provides challenges for usable security and privacy researchers. At the same time, rethinking research approaches provides an opportunity, as researchers might focus on aspects that were previously under-investigated or create new methods that might establish themselves as a new gold standard.

The presented list of approaches as well as the challenges and opportunities do not present but a selection of aspects in a research field that might receive more attention in the future. It is rather meant as a starting point towards more embracing approaches that take research out-of-the-lab into the real world.

ACKNOWLEDGEMENTS

Many ideas presented in this paper are a result of inspiring discussions with Albrecht Schmidt and Ville Mäkelä. Also, many researchers whom I worked with together contributed to the ideas, most notably Daniel Buschek and Mohamed Khamis. This work received funding from the DFG, grant no. 425869382 and from dtec.bw in the context of the 'Voice of Wisdom' project.

[2]Online Talkshow: How to do HCI reseach if your users are off limits? https://amp.ubicomp.net/users-off-limits/

[3]CHI'21 Course: Evaluation in Human-Computer Interaction – Beyond Lab Studies, https://hci-lecture.org/methods/

[4]IEEE Pervasive Computing–Special Issue on Out-of-the-Lab Pervasive Computing: https://www.computer.org/digital-library/magazines/pc/call-for-papers-special-issue-on-out-of-the-lab-pervasive-computing

REFERENCES

[1] Yomna Abdelrahman, Mohamed Khamis, Stefan Schneegass, and Florian Alt. 2017. Stay Cool! Understanding Thermal Attacks on Mobile-Based User Authentication. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) *(CHI '17)*. Association for Computing Machinery, New York, NY, USA, 3751–3763. https://doi.org/10.1145/3025453.3025461

[2] Florian Alt, Mateusz Mikusz, Stefan Schneegass, and Andreas Bulling. 2016. Memorability of Cued-Recall Graphical Passwords with Saliency Masks. In *Proceedings of the 15th International Conference on Mobile and Ubiquitous Multimedia* (Rovaniemi, Finland) *(MUM '16)*. Association for Computing Machinery, New York, NY, USA, 191–200. https://doi.org/10.1145/3012709.3012730

[3] Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2012. Increasing the Security of Gaze-Based Cued-Recall Graphical Passwords Using Saliency Masks. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Austin, Texas, USA) *(CHI '12)*. Association for Computing Machinery, New York, NY, USA, 3011–3020. https://doi.org/10.1145/2207676.2208712

[4] Daniel Buschek, Benjamin Bisinger, and Florian Alt. 2018. ResearchIME: A Mobile Keyboard Application for Studying Free Typing Behaviour in the Wild. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3173574.3173829

[5] Daniel Buschek, Alexander De Luca, and Florian Alt. 2015. Improving Accuracy, Applicability and Usability of Keystroke Biometrics on Mobile Touchscreen Devices. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1393–1402. https://doi.org/10.1145/2702123.2702252

[6] Daniel Buschek, Alexander De Luca, and Florian Alt. 2016. Evaluating the Influence of Targets and Hand Postures on Touch-Based Behavioural Biometrics. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (San Jose, California, USA) *(CHI '16)*. Association for Computing Machinery, New York, NY, USA, 1349–1361. https://doi.org/10.1145/2858036.2858165

[7] Mario Frank, Ralf Biedert, Eugene Ma, Ivan Martinovic, and Dawn Song. 2013. Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication. *IEEE Transactions on Information Forensics and Security* 8, 1 (2013), 136–148. https://doi.org/10.1109/TIFS.2012.2225048

[8] Michael Fröhlich, Maurizio Wagenhaus, Albrecht Schmidt, and Florian Alt. 2021. Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users. In *Proceedings of the 2021 ACM Conference on Designing Interactive Systems* (Virtual) *(DIS '21)*. ACM, New York, NY, USA. (to appear).

[9] Pascal Jansen and Fabian Fischbach. 2020. The Social Engineer: An Immersive Virtual Reality Educational Game to Raise Social Engineering Awareness. In *Extended Abstracts of the 2020 Annual Symposium on Computer-Human Interaction in Play* (Virtual Event, Canada) *(CHI PLAY '20)*. Association for Computing Machinery, New York, NY, USA, 59–63. https://doi.org/10.1145/3383668.3419917

[10] Mohamed Khamis, Anita Baier, Niels Henze, Florian Alt, and Andreas Bulling. 2018. Understanding Face and Eye Visibility in Front-Facing Cameras of Smartphones Used in the Wild. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (Montreal QC, Canada) *(CHI '18)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3173574.3173854

[11] Jonathan Liebers, Uwe Gruenefeld, Lukas Mecke, Alia Saad, Jonas Auda, Florian Alt, Mark Abdelaziz, and Stefan Schneegass. 2021. Understanding User Identification in Virtual Reality through Behavioral Biometrics and the Effect of Body Normalization. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI '21)*. Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3313831.3376840 liebers2021chi.

[12] John McAlaney and Peter J. Hills. 2020. Understanding Phishing Email Processing and Perceived Trustworthiness Through Eye Tracking. *Frontiers in Psychology* 11 (2020), 1756. https://doi.org/10.3389/fpsyg.2020.01756

[13] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (Glasgow, Scotland Uk) *(CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300340

[14] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2019. How well do my results generalize? comparing security and privacy survey results from mturk, web, and telephone samples. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1326–1343.

[15] Radiah Rivu, Ville Mäkelä, Sarah Prange, Sarah Delgado Rodriguez, Robin Piening, Yumeng Zhou, Kay Köhle, Ken Pfeuffer, Yomna Abdelrahman, Matthias Hoppe, Albrecht Schmidt, and Florian Alt. 2021. Remote VR Studies – A Framework for Running Virtual Reality Studies Remotely Via Participant-Owned HMDs. arXiv:2102.11207 [cs.HC]

[16] Albrecht Schmidt and Florian Alt. 2020. Evaluation in Human-Computer Interaction – Beyond Lab Studies. *Working Document* (2020). https://amp.ubicomp.net/wp-content/uploads/2020/04/Evaluation-in-Human-Computer-Interaction-Beyond-Lab-Studies.pdf

[17] Albrecht Schmidt, Ville Mäkelä, and Florian Alt. 2021. Evaluation in Human-Computer Interaction – Beyond Lab Studies. In *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems* (Yokohama, Japan) *(CHI EA '21)*. Association for Computing Machinery, New York, NY, USA, 1–4.

[18] Stefan Schneegass, Frank Steimle, Andreas Bulling, Florian Alt, and Albrecht Schmidt. 2014. SmudgeSafe: Geometric Image Transformations for Smudge-Resistant User Authentication. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (Seattle, Washington) *(UbiComp '14)*. Association for Computing Machinery, New York, NY, USA, 775–786. https://doi.org/10.1145/2632048.2636090

[19] Richard Shay, Saranga Komanduri, Patrick Gage Kelley, Pedro Giovanni Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2010. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) *(SOUPS '10)*. Association for Computing Machinery, New York, NY, USA, Article 2, 20 pages. https://doi.org/10.1145/1837110.1837113

[20] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. In *Proceedings of the 3rd Symposium on Usable Privacy and Security* (Pittsburgh, Pennsylvania, USA) *(SOUPS '07)*. Association for Computing Machinery, New York, NY, USA, 88–99. https://doi.org/10.1145/1280680.1280692

[21] Emanuel von Zezschwitz, Alexander De Luca, Bruno Brunkow, and Heinrich Hussmann. 2015. SwiPIN: Fast and Secure PIN-Entry on Smartphones. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (Seoul, Republic of Korea) *(CHI '15)*. Association for Computing Machinery, New York, NY, USA, 1403–1406. https://doi.org/10.1145/2702123.2702212

[22] Ding Wang, Qianchen Gu, Xinyi Huang, and Ping Wang. 2017. Understanding Human-Chosen PINs: Characteristics, Distribution and Security. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security* (Abu Dhabi, United Arab Emirates) *(ASIA CCS '17)*. Association for Computing Machinery, New York, NY, USA, 372–385. https://doi.org/10.1145/3052973.3053031