Interdisciplinary Human-Centered Security Research:
Learning From Opportunities and Challenges of a German Graduate Program

Jonas Hielscher
Ruhr University Bochum

Uta Menges
Ruhr University Bochum

Leona Lassak
Ruhr University Bochum

Hanna Püschel
TU Dortmund University

Olga Skrebec
Ruhr University Bochum

Christine Utz
*CISPA Helmholtz Center
for Information Security*

Abstract

Interdisciplinarity is a key aspect of Human-Centered Security (HCS) research to ensure that the human factor in security is considered from diverse perspectives. In this work we outline how graduate programs for HCS can be an enabler for successful interdisciplinary research. We reflect on SecHuman, a German HCS graduate program running since 2016, and summarize opportunities and challenges experienced by its two cohorts of PhD students. We outline the specific needs of interdisciplinary research in HCS and how institutions could create a supportive environment to meet them.

1 Introduction

HCS research often combines computer science, security, psychology, social sciences, and more [9]. However, the term *interdisciplinary research* has become an overused buzzword – working in an interdisciplinary team does not generate true interdisciplinary research by itself, as in the example of the computer scientist creating an app, which the psychologist then evaluates with users. The aim of interdisciplinary research is to generate new knowledge or to extend existing knowledge with insights from different disciplines [8, 10]. This can only be achieved through the process of knowledge integration, where relevant stakeholders draw on each other's perspectives to establish a common ground [5]. Effective knowledge integration can take up to years without methodological and institutional support, which is why a higher-level organization and instructional offerings at the individual and team level are essential [13]. Still, the result is worth the effort: Complex socio-technical (security) challenges can be addressed with socially robust knowledge that can be transferred into science and real-world practice. Specialized science in single fields, on the other hand, was found to generate fewer scientific breakthroughs [12].

In this report we present insights from SecHuman, an interdisciplinary HCS graduate program established by the German state of North Rhine-Westphalia at multiple institutions in the Ruhr area. Over the course of seven years, it funded a total of 25 PhD students from cybersecurity, computer science, psychology, law, educational science, mathematics, philosophy, electrical engineering, and linguistics. Here we introduce the program and – based on anecdotal evidence we collected from the PhD students – (self-)reflect on lessons learned as well as best practices identified over the last five years to inform future endeavors in interdisciplinary HCS research.

2 SecHuman

SecHuman [3] is a graduate school for interdisciplinary research in the space of cybersecurity. The first cohort (SecHuman I) started in 2016 and ended in 2021. The second (SecHuman II) began in April 2021 and is scheduled to conclude in 2024. Each cohort comprised twelve PhD students paired into six so-called "tandems." In each such pair, one student hails from a technical field – cybersecurity, computer science, or mathematics – and the other from a variety of different humanities or social sciences, including linguistics, psychology, science and technology studies, law, and anthropology. Each tandem is supervised by two, sometimes three Principal Investigators (PIs) from the respective fields and also paired with an external partner from industry or the public sector with the aim to foster transdisciplinary exchange, for example, through internships. One additional PhD student from psychology followed the process of interdisciplinary research from a meta-perspective. The tandems' PhD research was accompanied by a course "IT Security for the Humanities and Social Sciences" for the PhD students and PIs from non-technical fields and a second course that introduced the researchers from cybersecurity, computer science, and mathematics to core concepts and methods from the humanities, social sciences, psychology, and law. Bi-weekly seminars that either featured the SecHuman members' own PhD research or an invited talk provided the cohort with opportunities for networking and discussion. Annual symposia and spring or summer schools allowed the the tandems to present their work to industry partners, the research community, and the interested public.

1

3 Opportunities

The interdisciplinary approach in SecHuman provided its members with unique advantages and perspectives.

Available research methods: The pool of research methods grows with the number of fields involved. This can help to better understand the complexity of problems, allow for mixed methods that might better fit the problem, and interdisciplinary feedback can help to protect researchers from oversimplified conclusions.

Increased impact: As an applied science, security research [14] sometimes has the problem of limited impact in practice [7], for example, compared to medicine, where physicians often follow scientific news to consider new research in their own treatments. With interdisciplinary research and publication the audience naturally grows and so does the potential real-world impact. For example, SecHuman's reports in a techno-legal journal reached German policymakers and lawyers that would otherwise have been unavailable [15].

Interdisciplinary skill-building: The graduate school was accompanied by an interdisciplinary education program. The first SecHuman cohort mentored the second to share key experiences and challenges of interdisciplinary work in an intergenerative manner. The establishment of seminars, workshops, and summer or spring schools facilitated regular exchange between disciplines and encouraged doctoral students to engage in goal-directed scientific communication. Voluntary coaching on interdisciplinary collaboration in the research context enabled the PhD researchers to identify their individual challenges in the interdisciplinary work context to set goals for collaboration, develop strategies for dealing with ambiguity and uniqueness (in terms of different methods, vocabulary, etc.) in the interdisciplinary research process, among other aspects.

Multiple contact persons: In addition to their own tandem partner, SecHuman PhD researchers can benefit from the experience of people with different professional backgrounds. These include not only the tandem partner's PI, but also the other present and past doctoral researchers in SecHuman, who are available – with a lower inhibition threshold than in other cases – for questions, exchange, discussion, or networking.

4 Challenges

The PhD students in SecHuman also experienced several challenges unique to such an interdisciplinary context.

Mode of dissertation: In some disciplines, such as computer science and psychology, dissertations are built around previous conference or journal publications. By contrast, other fields like philosophy and linguistics require a monography, which means that no content that is influential to the dissertation can be published previously. These opposing requirements could become a major obstacle and in some cases hindered effective co-work.

Wanderers between two worlds: Reviewers do often not acknowledge research that prominently combines two different fields. A good example is the SecHuman tandem that worked on mental models of reverse engineers [2, 16]: The technical security community had its struggles with a *too soft* human perspective on a very technical problem, while psychologists did not understand why such a very specific population would need its own research.

No interdisciplinary education: Study programs are often missing education in research methods from other fields. Thus, skill sets which take years to be taught in a given method's mother discipline need to be adopted and comprehended by interdisciplinary researchers in a short period of time. This does not only put additional strain on the PhD students but also makes them more prone to errors in the application of methods and interpretation of results. This could only partly be prevented through the SecHuman coursework.

Overhead: Interdisciplinary work by its nature requires an understanding of each other's fields. To accomplish this understanding requires time, since one needs to become a semi-expert in a second discipline. Finding a common language between fields is challenging and time-consuming as well. Supervisors and institutions need to grant this extra time to prevent mental overload [1].

Differences in workload and compensation: In Germany, PhD salaries typically follow guidelines by the German Research Foundation (DFG) [6]. They contain field-specific tiers of compensation influenced by job prospects outside academia, leading to PhD students from the humanities being paid less than their peers from computer science and engineering. Adding to that, responsibilities outside SecHuman, such as teaching assignments, greatly varied between research groups. Still, everyone in the program was expected to complete the same graduation requirements within the same amount of funded time. To foster true interdisciplinary research, institutions should pay the involved researchers equally.

5 Takeaways

Interdisciplinary HCS research has the potential to solve novel problems – in SecHuman, for example, understanding the mental models of hardware reverse engineers [2, 16], (automated) authorship verification [4], or therapy for security professionals [11]. The key to success is methodological guidance to integrate diverse knowledge at every step of the research process. Successful interdisciplinary work can be achieved when institutions and research communities create frameworks that provide additional time and appreciative publication opportunities for content that is entrenched in more than one discipline. Moreover, common challenges, such as conflicting goals in the dissertation, should be communicated early and receive attention in the collaboration between PIs and PhD students.

Acknowledgments

References

[1] Zoë J. Ayres. *Managing Your Mental Health During Your PhD: A Survival Guide*. Springer Nature Switzerland AG, Cham, Switzerland, 2022. https://link.springer.com/book/10.1007/978-3-031-14194-2.

[2] Steffen Becker, Carina Wiesen, Nils Albartus, Nikol Rummel, and Christof Paar. An Exploratory Study of Hardware Reverse Engineering – Technical and Cognitive Processes. In *Proceedings of the Sixteenth Symposium on Usable Privacy and Security*, SOUPS 2020, pages 285–300. USENIX Association, 2020. https://www.usenix.org/conference/soups2020/presentation/becker.

[3] Ruhr University Bochum. SecHuman, May 2023. https://sechuman.ruhr-uni-bochum.de/, last accessed June 28. 2023.

[4] Benedikt Boenninghoff, Steffen Hessler, Dorothea Kolossa, and Robert M. Nickel. Explainable Authorship Verification in Social Media via Attention-based Similarity Learning. In *Proceedings of the 2019 IEEE International Conference on Big Data*, Big Data 2019, pages 36–45, New York, NY, USA, 2019. IEEE. https://doi.org/10.1109/BigData47090.2019.9005650.

[5] Rainer Bromme. Beyond One's Own Perspective: The Psychology of Cognitive Interdisciplinarity. In Peter Weingart and Nico Stehr, editors, *Practicing Interdisciplinarity*, pages 115–133. University of Toronto Press, Toronto, ON, Canada, 2000. https://doi.org/10.3138/9781442678729-008.

[6] Deutsche Forschungsgemeinschaft. Hinweise zur Bezahlung von Promovierenden (Guidelines for the Compensation of Doctoral Students), April 2023. https://www.dfg.de/formulare/55_02/55_02_de.pdf, last accessed May 26, 2023.

[7] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M. Angela Sasse. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *Proceedings of the 32nd USENIX Security Symposium*, USENIX Security '23. USENIX Association, 2023. https://www.usenix.org/conference/usenixsecurity23/presentation/hielscher.

[8] Julie Thompson Klein. Interdisciplinarity and Transdisciplinarity: Keyword Meanings for Collaboration Science and Translational Medicine. *Journal of Translational Medicine & Epidemiology*, 2(2), August 2014.

[9] Laura Kocksch and Andreas Poller. The Practice Turn in IT Security – An Interdisciplinary Approach. In Klaus David, Kurt Geihs, Martin Lange, and Gerd Stumme, editors, *INFORMATIK 2019: 50 Jahre Gesellschaft für Informatik – Informatik für Gesellschaft*, pages 97–98. Gesellschaft für Informatik, Bonn, Germany, 2019. https://doi.org/10.18420/inf2019_12.

[10] Veronica Boix Mansilla. Interdisciplinary Learning: A Cognitive-Epistemological Foundation. In Robert Frodeman, editor, *The Oxford Handbook of Interdisciplinarity*, pages 261–275. Oxford University Press, Oxford, United Kingdom, 2nd edition, 2017.

[11] Uta Menges, Jonas Hielscher, Annalina Buckmann, Annette Kluge, M. Angela Sasse, and Imogen Verret. Why IT Security Needs Therapy. In *Computer Security – ESORICS 2021 International Workshops*, ESORICS 2021, pages 335–356, Cham, Switzerland, 2021. Springer. https://doi.org/10.1007/978-3-030-95484-0_20.

[12] Michael Park, Erin Leahey, and Russell J. Funk. Papers and patents are becoming less disruptive over time. *Nature*, 613(7942):138–144, January 2023. https://doi.org/10.1038/s41586-022-05543-x.

[13] BinBin Pearce, Carolina Adler, Lisette Senn, Pius Krütli, Michael Stauffacher, and Christian Pohl. Making the Link Between Transdisciplinary Learning and Research. In Dena Fam, Linda Neuhauser, and Paul Gibbs, editors, *Transdisciplinary Theory, Practice and Education: The Art of Collaborative Research and Collective Learning*, pages 167–183. Springer Nature, Cham, Switzerland, 2018. https://doi.org/10.1007/978-3-319-93743-4_12.

[14] Jonathan M. Spring, Tyler Moore, and David Pym. Practicing a Science of Security: A Philosophy of Science Perspective. In *Proceedings of the 2017 New Security Paradigms Workshop*, NSPW 2017, pages 1–18, New York, NY, USA, 2017. ACM. https://doi.org/10.1145/3171533.3171540.

[15] Astrid Wichmann, Angela Sasse, and Christof Paar. IT-Sicherheit ist mehr als Technik. *Datenschutz und Datensicherheit*, 43(11):673–674, November 2019. https://doi.org/10.1007/s11623-019-1186-3.

[16] Carina Wiesen, Steffen Becker, Marc Fyrbiak, Nils Albartus, Malte Elson, Nikol Rummel, and Christof Paar. Teaching Hardware Reverse Engineering: Educational Guidelines and Practical Insights. In *Proceedings of the 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering*, TALE 2018, pages 438–445, New York, NY, USA, 2018. IEEE. https://doi.org/10.1109/TALE.2018.8615270.