Research Vision

The overarching vision of my research is improving the security and proper *operation* of distributed systems and networks. To realize this vision, I integrate my main methodological approach of developing and executing large-scale network measurements with an interdisciplinary combination of different fields to obtain scientific insights and provide actionable solutions that can improve the security and reliability of real-world systems. While network measurements provide me with empirical observations, real-world IT systems also contain a large organizational and social component. As such, a scientific approach towards understanding security and reliability in information systems must take an interdisciplinary stance, merging perspectives from the social (human factors) and political (governance) sciences with my core-contributions in network measurement.

Personal Research Approach: For my research, I take a unique approach that combines my practical experience as a system and network engineer to analyze systems with my background as a security and network measurement researcher incorporating a perspective on social, organizational, and societal components to obtain a holistic understanding of challenges for information systems' security. I use an analytical approach to *identify* study worthy effects. Once a potential effect has been identified, I utilize large scale network measurement techniques to assess the *impact* of the issue, and analyze the affected parties. Subsequently, I use methods from the social sciences to *explain* why the observed issue occurs, and then use the insights from the complete process to design *practical* solutions. Depending on the issue, these solutions may be *technical, organizational,* or *policy driven.* Finally, to complete the research cycle, I evaluate the efficacy of these solutions practice.

Past & Current Work: A major theme in my past research is the occurrence of (seemingly) 'simple' errors in code[1] and systems[2]. My past work in this area outlines how I converge my core methods from network measurements with human factors/societal perspectives to comprehensively work towards secure networked systems.

Security misconfigurations are a prime example of the interdisciplinary nature of security issues in information systems. While software engineers *have known* for years that untrusted input has to be validated and critical parsers should not run in the kernel context, we found that in the context of virtualized SDN components this paradigm is ignored in favor of more *functionality*[1]. Similarly, we know that resources should be decommissioned if they are no longer used. Still, we found that thousands of information systems are vulnerable to an attacker maliciously obtaining TLS certificates due to *forgotten* DNS entries pointing to cloud operators[3]. This work is also a good example of how my work connects to practice. We found an underlying issue in the ACMEv2 protocol, the protocol used by Let's Encrypt. Hence, in addition to the academic publication of these issues, we also present a practical solution that we actively contributed to the ACME working group within the Internet Engineering Task Force (IETF).

However, to assess the impact of such security misconfigurations, we must be able to measure them on the Internet. To make security misconfigurations measurable in the context of IPv6, I also made significant contributions to *scanning* the IPv6 Internet, something that is inherently difficult due to the larger address space in comparison to IPv4 (2^{128} instead of 2^{32} possible addresses)[3,4]. In addition, I recently contributed to the formalization of the asset discovery process[5] and created new methodology to identify forgotten websites on the Internet[6].

---

[1] Thimmaraju, K., Shastry, B., **Fiebig, T.**, Hetzelt, F., Seifert, J. P., Feldmann, A., & Schmid, S. (2018). Taking control of SDB-based cloud systems via the data plane. In ***Proceedings of the Symposium on SDN Research (SOSP)***.

[2] Borgolte, K., **Fiebig, T.**, Hao, S., Kruegel, C., & Vigna, G. (2018). Cloud Strife: Mitigating the security risks of domain-validated certificates. In ***Proceedings of the Network and Distributed Systems Security Symposium (NDSS)***.

[3] **Fiebig, T.**, Borgolte, K., Hao, S., Kruegel, C., & Vigna, G. (2017). Something from nothing (There): Collecting global IPv6 datasets from DNS. In ***Proceedings of the International Conference on Passive and Active Network Measurement*** (pp. 30-43). Springer

[4] Borgolte, K., Hao, S., **Fiebig, T**., & Vigna, G. (2018). Enumerating active IPv6 hosts for large-scale security scans via DNSSEC-signed reverse zones. In ***Proceedings of the IEEE Symposium on Security and Privacy (Oakland)*** (pp. 770-784).

[5] Vermeer, M., West, J., Cuevas, A., Niu, S., Christin, N., van Eeten, M., **Fiebig, T.**, Ganan, C.H., and Moore, T. (2021). SoK: A Framework for Asset Discovery: Systematizing Advances in Network Measurements for Protecting Organizations. In ***Proceedings of the 6th IEEE European Symposium on Security & Privacy (EuroS&P)***, 2021.

[6] Pletinckx, S. R. G., Borgolte, K., and **Fiebig, T**. (2021). Out of Sight, Out of Mind: Detecting Orphaned Web Pages at Internet-Scale. ***Proceedings of the ACM SIGSAC Conference on Computer and Communications Security***.

Finally, I combine insights from my technical work with methodology from the social sciences to synthesize *understanding* and *explain* why avoidable errors occur. To understand why systems in practice turn out not to be secure or sufficiently privacy preserving[7]. In sum, this prior work highlighted the importance of human and organizational factors in the proper operation of distributed systems, and led me to also seek solutions for IT security challenges in and interdisciplinary perspective, incorporating the domains of policy[8,9] and governance[10] to find a functionally safe and secure approach to building information systems.

Vision for the Future: For my future work, I will continue my work on measuring, explaining, and mitigating operational security issues in the domain of distributed systems, for example, by continuing my investigation of orphaned resources on the Internet. I will also continue to converge technical perspectives with policy related dimensions, as I did in the context of digital sovereignty and privacy in my recent work on higher educations' reliance on cloud computing infrastructure, and what this means for lecturers and teachers in terms of dependence and academic freedom[9].

Furthermore, in support of the vision of my PhD student Mannat Kaur for this perspective, I am working with her on a feminist perspective in the security of IT systems—for example the impact of toxic masculinity on risky behavior when operating systems (skipping four-eyes rules etc.)—where I see great opportunities for future research in the context of usable security, but also in the context of utilizing network measurements to quantify the impact of cultural challenges in IT operations.

In summary, my vision for the future is using network measurements to address the pressing issues in the field of Information Systems' Security in all its breath, converging measurement results where necessary with perspectives from IT security, privacy, human factors, and social and societal dimensions. To attain this goal, I collaborate with my national and international network to form effective collaborations to tackle one of the most urgent questions of my time: How do we build and maintain secure and dependable Information Systems that benefit society, instead of introducing new threats and challenges, while subsequently mitigating those threats and challenges already present?

Research Funding and Collaboration: My research and funding activities strongly benefit from my large national and international network, both in industry and academia. My role as the leader of the governance work package in the H2020 CyberSecurity4Europe project and close collaboration with Prof. Rannenberg from Goethe University Frankfurt as the overall PI of the project, my activity in industry organizations like the IETF, and my participation in program committees of major Network Measurement (ACM IMC, ACM CoNEXT) and security venues (ACM CCS, IEEE S&P, RAID, USENIX Security) have significantly contributed to the growth of my network. I plan to continue to expand this network, and work with my national and international partners, both to obtain funding and develop my research agenda.

---

[7] Dietrich, C., Krombholz, K., Borgolte, K., & **Fiebig, T.** (2018). Investigating system operators' perspective on security misconfigurations. In ***Proceedings of the ACM SIGSAC Conference on Computer and Communications Security***.

[8] **T. Fiebig**, How to stop crashing more than twice: A Clean-Slate Governance Approach to IT Security, 2020, In ***Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)***, pp. 67-74,

[9] **Fiebig, T.** et al. *Heads in the Clouds: Measuring the Implications of Universities Migrating to Public Clouds.* arXiv preprint arXiv:2104.09462.

[10] Sterlini, P., Massacci, F., Kadenko, N., **Fiebig, T.**, & van Eeten, M. (2020). Governance Challenges for European Cybersecurity Policies: Stakeholder Views. ***IEEE Security & Privacy***, *18*(1), 46-54.