

Janosch Maier
Konrad-Celtis-Str 84
81369 München
☎ +49 89 839310197
✉ maierjanosch@gmail.com

Research & Teaching Statement

The goal of my research is, to make information technology more secure. Not for the sake of secure services, but for users who rely on software to use their data carefully. In today's connected society, we are able to do almost everything online: shopping, banking, dating, communicating, ... Most parts of our everyday life would be different without the use of automated data processing tools. Security breaches in such systems harm not only companies or institutions in terms of image or revenue, but also the users who trust those entities to have secure systems in place.

1 Application Security

Application security includes several different fields of work. Where penetration testing may uncover vulnerabilities of an application or the underlying system, code reviews and other quality measures might have prevented those beforehand. Security is a tradeoff between what data I need to secure, and how much effort I can put in, implementing security measures. In my bachelor thesis [3], I identified vulnerabilities in the operating system design of Android and evaluated countermeasures. The proposed system to separate private and company content on a smartphone is used by technologies like Samsung KNOX¹. On the Droidcon London 2013, I shared² my research with the Android developers community. SecureLinux is part of the mainline Android Kernel by now. Sensitive data may not only be secured by means of secure system design or encryption. In some cases such as statistical surveys, data should only be collected in anonymized form. However, when collecting data even with the best intentions, deanonymization is possible in certain cases. Anonymization models show, which attacks can be prevented when a certain form of anonymity is in place [1, 2]. Toolboxes may help to put data into an anonymized form before releasing data for the public.

2 Human Device Interaction

Technical security measures are only as good, as the user wants them to be. Security alerts, that users do not read, fail their purpose. Why try to break into a system with technical means, when you can just ask

¹<https://www.samsung.com/de/business/solutions-services/mobile-solutions/security/samsung-knox/>

²<https://skillsmatter.com/skillscasts/4616-hardening-android-dual-boot-for-enterprise-usage>

the user for his password; And receive it? Occasionally, users need training to be aware of certain security risks. For general purpose, systems should be implemented in a way, that states to the user, if their is a security risk. Not train its users to verify all alerts without reading. As a student volunteer at the conference “Mensch und Computer” (Human and Computer), I helped bringing those two fields of research together. As a research assistant at Ludwig-Maximilians Universität München, I do data collection and analysis at the institute of General Education and Educational Research. Online data collection tools are a basis for the ongoing research here.

3 Social Implications

Educational research is highly related to research fields from computer science. Findings from research about big data or knowledge management systems, influence, what people know and how they learn. Computer supported collaborative work takes a look at group dynamics, and applies those theories to groups with different group awareness and completely different methods in communication. Online learning e.g. through MOOCs, introduces forms of information sharing only possible through our technical progress. I also take a look at social structures not only from the computer scientist's, but the educational scientist's view [4]. Research on the comparison of presentation programs due to the existence of graphical organizers will be presented in spring 2015.

4 Database Systems

I have been tutor for the introductory course database systems at Technische Universität München for several years. Database systems are the basis for many applications. Their understanding is not only important for using those systems, but also noticing their security implications. I try to encourage my students to critical thinking about software systems. Group works help the students to foster their thoughts about the lecture topics. This enables them to state their position in front of the bigger crowd of their colleagues. I try to highlight the relevance of certain topics, by relating exercises to real world examples. As database systems are always in the background of larger software systems, their relevance can be easily understood by looking at the services, a database delivers in typical software scenarios.

5 Future Research

In the future, I will try to bridge the gap between computer science and social sciences. Looking at how technical security measures influence user behaviour. How can vulnerabilities, that originate from social engineering attacks, be fixed? Here technical means have to work hand in hand with training and awareness raising. How can these benefit from each others efforts, without multiplying work, but foster each other?

References

- [1] J. Maier. *Anonymity in Networks I - Basics*. seminar paper, Technische Universität München, München, Jan. 2012.
- [2] J. Maier. Anonymity: Formalisation of Privacy – k-anonymity. In G. Carle, M.-O. Pahl, D. Raumer, L. Schwaighofer, U. Baumgarten, and C. Söllner, editors, *Proceedings of the Seminars Future Internet (FI), Innovative Internet Technologies and Mobile Communications (IITM) and Autonomous Communication Networks (ACN), Summer Semester 2013, volume NET-2013-08-1 of Network Architectures and Services (NET)*, München, 2013. Chair for Network Architectures and Services, Department of Computer Science, Technische Universität München.
- [3] J. Maier. *Enhanced Android Security to prevent Privilege Escalation*. Bachelor thesis, Technische Universität München, 2013.
- [4] J. Maier. *Sozialisation durch Gleichaltrige*. Coursework, Ludwig-Maximilians Universität, 2014.