Get to know Thorsten Strufe

Interview + Transcription: Jennifer von Olnhausen

Scientist: Thorsten Strufe

[smoothed transcription]

So, you're asking about the history of the chair:

This chair was created as a new professor position in 2019, essentially by the KASTEL institute, to establish a little bit more competence in the context of privacy and practical security matters. My own history is that I was an assistant professor at TU Darmstadt, for distributed systems, or reliable dependable systems, and subsequently I was a full professor at TU Dresden for privacy and IT security in general, and essentially the idea was that I could join and provide a little bit more background, or experience, with regards to the practical or empirical side of security and more background on privacy, network security and other practical aspects of security.

So, your question is, what we are currently working on:

And I take this 'you' as us, the entire group at the chair.[1] So, here at the chair we have two lines of activities, one line is 'really' systems and network security, where we're thinking about ways that communication on the networks, or the networks themselves, can be protected from attacks. The second line of research, which makes up for the majority of activities of the chair at the moment, really deals with privacy, and here again we have two lines of research: one line of research is trying to understand behavioral privacy. So, the situation is, of course, that with increasing digital transformation and increasing numbers of devices around us, we are observed more and more by digital systems. And we try to figure out to which extend such kind of observations can actually break the privacy of individuals/of citizens. Why would that be interesting? So, of course if you're playing games, maybe you're wearing gloves or wearable devices, or you're using controllers, but also when you're walking through a shopping mall or around town, then smart devices around you are recording what you're doing, where you're going and so on. Of course, this can provide lots of novel services, so it has many benefits, on the other hand, it may so happen that such kind of recordings or observations would give away information that you don't really want to share with others. So, first of all, it could be that you have information in the data that is identifying individuals, so, that people can be reidentified, but also it could happen that data is contained in such kind of observations that would allow for inferring sensitive information like medical conditions or preferences or different other types of private information.

And then in a second line of research, we're actually trying to protect the citizens by building privacy enhancing technologies. We are working on anonymous communication to allow people to use the internet freely with liberty, and we're also thinking about building privacy

[1] The original question was: what are you currently working on?

enhancing technologies that would allow people to use such kind of, let's say wearable devices or modern IT systems, maybe the metaverse, without leaking information that they do not want to share with others.

So, your third question is: 'What do we want to achieve with our research?'

And that's a really nice question, and I think that there are two main motivators that drive us. One motivator is that we like technology and that we like to understand what is possible and how we can push the parcel, how we can push the limits, how we can make things that were previously thought to be impossible. We were talking about privacy in the sense of inference, where we are mainly interested in the inference of private information, but of course it's also interesting to consider what is possible with machine learning or AI, in the sense of improving services or improving insights.

So, our second motivator is maybe slightly more ethically driven: if we look at the development of the digital ecosystem, then we realize, that this is mainly pushed by large institutional players. And if you think, e.g., the companies are developing lots of new services, which are useful and interesting for the costumers (or for users), then their main driver is to make profit. And unfortunately, this profit can be increased by reducing costs, and this very often comes at the cost of the privacy of the users or the individuals. Also, when we think about institutional players like government agencies, maybe law enforcement agencies, then, of course, their primary purpose is to investigate crimes, and this is made much easier if they establish a large surveillance infrastructure.

While we understand their relevance and while we understand why they would like to have such kind of infrastructures, we believe that this actually is detrimental to society and we also see at the same time that individuals or the citizens don't have much of a lobby, and that's why we try to show to which extend such kind of activities interfere with the privacy as a human right, as well as how the privacy can be improved for individual citizens.