Get to know Christoph Coijanovic

Interview + Transcription: Jennifer von Olnhausen

Scientist: Christoph Coijanovic

[smoothed transcription]

How did I get here?

Well, I finished both of my bachelor's and master's degree in Computer Science here at KIT and during my master's of course I very much tried to focus on cryptography and IT-Security, so naturally, when it came to write my master's thesis, I also was looking for a topic in that direction. And at that time the Chair of Privacy and IT-Security was quite new at KIT, so no one really knew about them. Well, then they advertised one of their topics over the Krypto-mailing-list and that's how I found out about them. Although I kind of came to them by accident, I very much enjoyed my topic and indeed, I enjoyed it so much that I just stayed on and continued my research.

What am I doing at the moment?

Currently I'm focusing on the Signal instant messaging app, especially on Signals group management. Imagine you're in a Signal group, then of course you need a way to learn who the other group members are, and also you maybe want to add group members or remove them again. For that, Signal has come up with a pretty clever protocol where group membership is managed by a central server but that server doesn't actually learn who the group members are. But what we found that it does learn, is a member's index within the membership list. Imagine you're trying to access the group membership list, then the server learns that you are, for example, the second member within the group. And now, if you later come again and want to do some other operation, the server learns 'ah, that has been the same user as before', of course this can be a privacy risk so we're trying to improve the situation. And to do so, we first need to formalize which information actually is disclosed, then we're trying to propose an improved protocol, and then we can use our formalization to rigorously prove that our protocol is actually better than the state of the art.

What are my research goals and plan for the future?

In general, I do want to understand the particularities of anonymous group communication. For example, what is the privacy sensitive information and what are the challenges in trying to protect it? Of course, also I do want to use this knowledge to build better protocols because as you know, most people use group communication every day, for example with Signal as we talked about but also Slack or Microsoft Teams and at that kind of scale, the existing solutions for anonymous group communication simply wouldn't work, so, we do need to come up with better protocols in the future.