Speaking the language of privacy

What does privacy really mean in a time when a lot of personal information is collected and stored on a daily basis? How do software developers actually respond to privacy issues? Gabriele Lenzini wants them to be able to formalise these aspects in a generic way. To this end, he is developing a language.

Gabriele Lenzini

'Security is an issue of ever growing importance. But what about privacy? Security and privacy are sometimes linked, for instance, when we talk about the security of personal information. At other times, they seem to be in opposition. Privacy aspects have always been addressed using an ad hoc and largely restrictive approach. We are now trying to find solutions, which offer a more general way to protect the confidentiality of data. Although I have worked on security protocols and their mathematical descriptions, privacy, in this respect, will be a new topic for me. Can we assess the quality of software or a complete system as to their privacy aspects? As part of the PAW (Privacy in an Ambient World) project, my first aim is to describe these issues by means of a mathematical language. Expressing privacy requirements and policies using a formalized mathematical language, thereby obviating semantic ambiguities, is an essential step if we want to develop tools or strategies to help evaluate the privacy of systems.'

'The number of systems and organizations collecting and storing information about us increases rapidly on a daily basis. This is not just about sensors and cameras, it also includes the information you provide by simply using your mobile phone or whenever you present your loyalty cards at the supermarket. Each time you provide very useful information. With the information provided, supermarkets can track potentially interesting trends in your shopping choices. What if the supermarket were to sell the information about your lifestyle to insurance companies? Another situation involves the rapid exchange of medical data in emergency situations. How can you be certain that a doctor only accesses your files when it's truly necessary? This could potentially be solved through the definition of licences. I want to describe these aspects mathematically, developing a model and a language to provide designers with tools to check on privacy policies. In short, what information is allowed to be seen and by whom?'

'The CTIT's broad scope can be advantageous were as well. We have the opportunity to work together with sociologists in this field. Even though our work as computer scientists primarily concerns issues related to the formal description and analysis of privacy, the problems surrounding privacy reach across different levels and involve different entities of modern society. There are, however, gaps to be bridged in this respect. You could take the issue a few steps further to include the legal aspects, but that is beyond my scope. Besides, law only comes in after something has gone wrong.'

'Taking this approach, we are also trying to develop a formal framework within which the work performed by data managers is recorded in some protected way to enable checks at a later stage to see whether they have complied with the privacy policies they claim to maintain. The check could be, for example, required by the law in instances when there is a suspected violation of privacy.'

Project examples:

- LicenseScript (Telematics Institute)
- BioSecure (EU/FP6)
- BASIS: Biometric Authentication Supporting Invisible Security (IOP-GenCom)
- Secure Grip (STW)
- Privacy in an Ambient World (IOP-GenCom)
- INSPIRED: Integrated Secure Platform for Interactive Personal Devices (EU/FP6)

‘In my opinion, the interdisciplinary approach is the project’s most attractive aspect. I like co-operating with actual developers to “stay sharp”. At the same time, the semantics of a language, aesthetics of a model and the mathematical descriptions truly pique my interest. This preference also manifested itself in the work I did in Italy, when I worked on the development of formal methods and on biological computation. In addition, I completed a project at CTIT in 2002, made possible by a research grant. This was one of the reasons why I wanted to return to Twente for the PAW project.’