Systematic Analysis of Security Protocol Implementations

11- 15 June 2018 Lorentz Center @ Oort

Security protocols play an important role in our everyday lives, for example, when paying with our contactless bank cards, calling using our smartphones, or making use of online banking. The goal of this workshop was to bring together researchers from different areas to improve the analysis of the implementations of these types of security protocols. To achieve this, the participants worked together in small groups on concrete use cases to see how their different expertises could be combined. These case studies were brought in by the participants.

At the beginning of the week the case studies were presented by the selected group leaders. In the following one-hour session participants had an opportunity to discuss the case studies with the respective group leaders. Afterwards, participants could choose a case study to work on. The rest of the week we started in the morning with a couple of presentations on new attacks or novel methodologies in the area of protocol analysis. In the afternoons, the main focus was to work in groups on the selected case studies. Short plenary sessions were held during the week to discuss the progress in these groups. This approach was appreciated by the participants and everyone was very actively working in their groups.

During the week the basis was laid for various new projects and collaborations. This included, for example, the formal analysis of new WiFi handshakes, analysis of new side-channels in TLS implementations, the application of new analysis methods for WiFi and LTE devices, as well as the analysis of smart card applications. Bringing together different communities had a very positive effect on the collaborations. The TLS working group could analyze new padding oracle attacks with the help of model-based testing techniques provided by the LearnLib developers. The WiFi group was able to prove specific aspects of selected protocols with the help of the invited WiFi experts. The LTE group made some first steps towards the analysis of state machines implemented in mobile phones. All these analyses were only possible thanks to the availability of researchers from different communities: state machine learning, model-based testing, cryptography, and security protocol implementation.

Given the positive feedback of our participants and the interdisciplinary aspects of our groups, we await high-quality publications coming out as results of our workshop. According to the last information from our participants, the work is still ongoing and there are intentions to publish the results.

We would like to thank the Lorentz center for providing us the possibility of organizing this workshop. The feedback from our participants motivates us to start planning the organization of a follow-up next workshop, for which we plan to use the same workshop format.

Joeri de Ruiter (Nijmegen, Netherlands)
Juraj Somorovsky (Bochum, Germany)
Frits Vaandrager (Nijmegen, Netherlands)