Summer School on Real-World Crypto and Privacy Travel Report

June 5-10, 2016, Sibenik (Croatia)

By: Ilir Bytyçi, PhD cand., Department of Telematics, NTNU

For: COINS - Research School of Computer and Information Security

Sponsored by: COINS

Report

This report will describe the travel report from the Summer School on Real-World Crypto and Privacy held in Sibenik, Croatia, between 5-10 June, 2016. The venue of the summer school was in Solaris Resort, which is outside the city of Sibenik, close to the seaside.

1. Summer School on Real-world Crypto and Privacy

The summer school was jointly organized by the Digital Security (DS) group, Radboud University, The Netherlands, Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia, the COSIC group, KU Leuven, Belgium, and ETH Zurich Information Security and Privacy Center, Switzerland. The summer school's aims were at bringing together PhD students (especially those at the beginning of their PhD), postdoc researchers and security experts from industry. It was a great opportunity to meet with researchers from the common field of research as well. Well-known cryptographers were also lecturing, among them, Joan Daemen (one of the inventors of AES competition winner - Rijndael), Phillip Rogaway, Bart Preneel, Dan Bernstein.

2. What to Expect

The summer school topics varied, however, the main topics included introductory level as well as advanced discussions on:

- Secure hardware and physical security
- Cryptography for the Internet
- Formal methods in cryptography
- Wireless security
- Crypto for systems security

- Privacy enhancing technologies
- Traffic analysis and countermeasures
- Recent developments in symmetric-key crypto

Full program of the summer school, as well as presentation slides can be downloaded from the webpage of the program. [1]
Some students who applied early in time could benefit from stipends offered by the organizers.

3. Brief Description of Topics Presented

During the summer school, topics discussed varied from speech to speech. The summer school was opened by a speach on symmetric encryption, by one of the Rijndael algorithm inventors, Joan Daemen. Next speech gave an overview of usage of elliptic curves for public-key constructions. After lunch, another different discussion was initiated, this time on side channel crypto-analysis, and later an accompanying hardware encryption tutorial (using the Xilinx platform)

The second day started with an interesting topic on how secure positioning works, and what are threats to GPS and proposals how to improve the situation. After that, there was a session on blockcipher security notions. Formal proofs (crypto-aided) of crypto-primitives by IMDEA Software Institute, together with the interactive proof assistant - EasyCrypt was presented. Then the world famous prof. Rogaway gave a two-part session on Authenticated Encryption. The second day ended with an introduction to symbolic verification methods, where the Scyther tool was briefly demonstrated.

No lectures took place on the third day, as an excursion was organized for the interested participants. For some it was an opportunity to visit the old city of Sibenik instead.

Parallel sessions started on the fourth day, touching upon topics on symmetric and asymmetric encryption, as well as privacy. The topic which atracted my attention the most was on TLS export cipher attacks by Heninger and Halderman. They presented the latest attacks on TLS such as Logjam, FREAK and the factors contributing to such attacks, by last sharing also remediation proposals to prevent these attacks.

On the last day, parallel sessions continued, from which I attended those

[1] http://summerschool-croatia.cs.ru.nl

related to network security, namely discussions on security of SSH by Kenny Paterson, and security issues with DNS by Dan Bernstein. The last day concluded with interesting presentation of Tor by Roger Dingledine, and last lecture I attended was on advanced protocol verification methods, where Tamarin tool was presented, a tool which attempts to include human factor in the modelling of crypto protocols.

4. Personal Benefits and Conclusion

The summer school did not include topics very closely related to the field of study I am closely involved in, homomorphic encryption (HE) or how to secure emerging network technologies using the latter. However, as a new PhD student it was very useful to look at various topics that are related to securing network communications, and ensuring privacy of communications, as well as various topics in cryptography as a field. It was an opportunity to meet at least two PhD students who were also doing research close to the field of my research, both looking at practical uses of HE at protecting health data.

Last but not least, during the summer school, it was also possible to meet well-known cryptographers such as Prof. Philip Rogaway, whom we invited to make a visit to NTNU and Norway, and he promised to do so in autumn. If this visit is organized by us, then it will be an opportunity for NTNU to organize a workshop or a wider discussion on privacy, with prof. Rogaway being an honored guest lecturer.