Reflection report from the 2016 COINS Summer school on Authentication

Martin Strand (martin.strand@math.ntnu.no), August 2016

The 2016 Summer school on authentication was my first pure COINS event, and gave new insights on a wider part of the field that COINS covers. During the week in Greece, we had in total four speakers covering topics such as balancing usability and authentication, the new EU regulation eIDAS (and identification federation in general), mobile network authentication and network forensics. Unfortunately, a fifth speaker had to cancel his presentation due to technical problems.

I did not participate on the visit to ENISA ahead of the summer school.

One of my main lessons from the week was that there exists a big gap between cryptography and information security. The gap manifested itself several times. I will give two major examples.

- In cryptography, at least among theoreticians, a scheme is considered insecure when it can no longer be considered completely secure, for instance due to the existence of an attack. This binary view was challenged by one of the speakers. His belief was that one should also consider risk, and a spectrum of security, where the scheme is judged based on requirements, organisational measures, degree of security and the consequences of an attack in practice. While I disagree for the concrete example in the discussion, it still is a useful aspect to consider.

- Information security and cryptography occasionally use widely different definitions for the same concepts, for example what is meant by "identification" and "authentication". For the former, authentication is the stronger concept, whereas identification is a weaker notion that can be achieved without user activity. For cryptographers, it is almost the other way around: Authentication means that "A can prove to B that he is A, but someone else cannot prove to B that he is A", while identification is stronger: "A can prove to B that he is B, but B cannot prove to someone else that he is A"[1].

These differences are not necessarily a problem on their own, and it is not obvious which is better, but there is clearly need for some work mitigating

[1] Amos Fiat and Adi Shamir. How To Prove Yourself: Practical Solutions to Identification and Signature Problems (1987)

these cultural differences, so that the mathematicians and cryptographers who develop novel schemes can communicate in a precise manner with those who might implement and use the solutions. The other way around, programmers and system architects need to be able to explain real world (although not completely fatal) attacks to cryptographers in a useful way.

Wednesday was spent on "non-curricular activities" – i.e. an excursion to the northern part of the island. The better part of the day was spent in Mithymna, with a visit to a castle with roots back to the Trojan war. The fortification on the top of the hill played a strategic role until just a few hundred years ago.

It is easy to underestimate such social days. However, they are crucial for networking and getting to know potential collaborators. Personally, I got a couple of interesting tips during the week, although none of them seems to be sufficient for papers from my side. My primary benefit from this summer school will probably not be clear until I apply for a job in the industry.