Norwegian Information Security Conference (NISK) 2018
Reflection report

Nikolay Kaleyski

December 5, 2018

1 Background

The eleventh Norwegian Information Security Conference (NISK) took place in Longyearbyen on the Svalbard archipelago. The event was remarkable for many reasons, not the least of which was the unusual location which I consider to be one of the most interesting and exotic places I have visited thus far. Visiting Longyearbyen allowed me to experience both the cold breath of northern nature, and the warm comfort and hospitality of a secluded but functional community. The conference itself was unusual as well, as it combined several events in one place: the COINS Ph.D. student seminar took place on September 18, in which several of my fellow doctoral candidates from around Norway gave talks on various topics related to their studies, and was followed by NISK, NIK, UDIT and NOKOBIT conferences on September 19 and September 20 which took place in parallel. The topics of the presentations were quite varied, giving one a taste of different venues of research in the fields of Computer Science and Information Security.

The organization of the conference was outstanding, and a sufficient amount of free time and social activities were provided by the organizers so that the participants could enjoy the unique atmosphere of Svalbard as fully as possible during their short stay in addition to the scientific and social aspect of the event.

I am grateful to COINS for providing the financial support allowing me to visit such an amazing place and to expose myself to the ideas of researchers from so many different branches of computer science and information security.

Below I give a brief overview of some of the presentations given at NISK. The full program of the event along with other useful information, including the conference's proceedings, can be found at `http://nikt2018.ifi.uio.no`.

2 Overview of Selected Talks

2.1 Talks at the student seminar

As mentioned above, the COINS Ph.D. student seminar took place on the day before NISK; it allowed, among other things, recent graduates from their studies at COINS universities to share their (non-necessarily scientific) experiences and advice. Two particularly interesting such talks were given by Bo Sun and Chris Carr, entitled “There is always light at the end of the tunnel” and “How to get (and not to get) a PhD + why you should / shouldn’t travel”, respectively. Two of the biggest challenges facing any doctoral candidate are certainly the stress and uncertainty, and the difficulties in managing his time and dividing his energy and efforts between different activities. The two talks aimed at exactly these problems and, collectively, provided advice and reassurance to anyone undergoing the same process.

2.2 Talks at NISK

On the first day of the conference, Martha Norberg Hovd gave a rather interesting talk entitled “A Successful Subfield Lattice Attack on a Fully Homomorphic Encryption Scheme”. As the title of the talk suggests, the topic concerns lattice-based cryptography, and an encryption scheme based on the NTRU cryptosystem in particular, which is somewhat different than the encryption techniques I am familiar with, but is nonetheless intriguing as it constitutes a different approach to using mathematical structures in the design and study of cryptographic algorithms. Briefly put, it is shown that a fully homomorphic scheme based on NTRU is susceptible to the subfield lattice attack, which is inherent in the structure of the scheme.

Another engaging talk was “Fake Chatroom Profile Detection” which presented work by Patrick Bours, Parisa Rezaee Borj and Guoqiang Li from NTNU. The authors’ research focused on identifying chatroom users that assume fake identities by means of biometric keystroke dynamics and stylometry. The practical implementation of the techniques is done by means of a support vector machine (SVM) which was trained on keystroke dynamics data gathered from NTNU’s students and staff. This results in a surprisingly high accuracy of detection even with a very small amount of chat messages available. While the authors mention that including stylometry into their framework is still a topic for future work, the results already obtained look quite promising and are especially intriguing due to their practical relevance and utility to modern society.

Of course, there were many other talks given, and participants were also allowed to present their research and ideas with posters between the conference’s sessions. I prefer, however, to constrain myself to the two talks above due to the very large number of interesting presentations at the conference.