Nikita Karandikar
PhD Candidate
University of Stavanger
Supervised by: Antorweep Chakravorty, Chunming Rong

NISK Reflection Report

18th September COINS Workshop

The COINS workshop started with a welcome speech and round of quick introductions. The first segment was called **'Lessons learnt from doing a PhD'**. The presenters **Chris Carr, Andrii Shalaginov** and **Bo Sun** shared their experiences with their PhD. Chris described the challenges with maintaining work-life balance and offered some tips to help. I found the tips quite useful especially the recommendation to submit a draft to the supervisor as soon as you have one instead of trying to perfect it too much. Andrii also spoke about work life balance and the challenges of trying to fit all the commitments of a PhD into a 37.5 hour work week. Bo spoke about her journey through a PhD by presenting pictures of her best and worst moments and talking about the difficulties she faced and how she overcame them.

This was followed by technical presentations by current PhD students. **Adam Szekeres** spoke about predicting human individual decision making in the context of IoT security and I found the study about CEO profiling with IBM Watson quite interesting. **Ali Khodabakhsh** spoke about fake news detection by means of biometric and presentation attack detection and ended by contrasting the ability of humans to machines in this context given various scenarios. **Jan William Johnsen** gave a talk about identifying central individuals in organized criminal groups. **Mazaher Kianpour** talked about quantifying risk vs gain and managing security and insecurity externalities. This was followed by **Muhammad Mudassar Yamin** whose talk focused on cyber security exercises and his focus on knowledge improvement in operation and focus to reduce time required to implement for cyber security exercises. The last presenter of this segment was **Shukun Tokas** who focused on language based mechanisms for GDPR compliance.

The next segment called Life after PhD had two presenters **Berglind Smaradottir** and **Bikash Agrawal**. Berglind spoke about the challenges of getting an academic position after PhD and also mentioned some jobsites one may look at. Bikash talked about his experience of creating a startup and presented the workflow of idea to product to creating a team to execution.

This workshop ended with election of two COINS student representatives.

19th September Presentations

The day started with an opening by **Ellen Munthe-Kaas**, Head of Department UiO, followed by a keynote speech by **Prof. Barbara Wasson** leader of SLATE at the Longyearbyen Kulturhus. Prof. Wasson started with an overview of SLATE (Centre for Science and technology). She then moved on to Learning Analytics and presented a state of the art on the subject. Learning Analytics is the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs. We then looked how learning analytics enables adaptive

learning systems. She elaborated on the role of Learning analytics in predication and retention, prediction of performance, student/teacher behavior modelling, increasing self-reflection and self-awareness, improving assessment and feedback and others. She then mentioned some selected projects such as the AVT project and then summarized.

We then went around and saw the poster presentation. There were some interesting posters like '**NEST instrumentation app**' and '**Simulating brain scale neuronal networks on exascale computers**'.

There was a segment called **'Cryptoprimitives'** with three presentations. **A successful subfield lattice attack on fully homomorphic encryption scheme** talks about NTRU and FHE schemes. It presents a FHE that needs the additional operations KeySwitch and ModSwitch to be fully homomorphic. **Improving the generalized correlation attack against stream ciphers** which presents a solution for generalized correlation attack using constrained approximate search and bit parallel implementation. The third presentation had to be rescheduled to the end and it was on **debunking Blockchain myths**. The presenter talked about 7 myths including those about storage technology, mining, private blockchains and others. As my current work focusses on blockchain, this presentation was of particular interest to me. There was then a keynote speech by **Elise K. Lindberg** which was followed by a break and poster presentations.

The second segment called **Cryptoprotocols** had two presentations. **Distributed personal password repository using secret** started with existing technical solutions, the concrete protocol, details of the pilot experiment conducted and a conclusion. **The tension between anonymity and privacy** started with the importance of GDPR and moved on to a sequence of ad-hoc patches, syntactic or checkable privacy, deterministic sanitizer, counter examples and differential privacy.

Before the last segment, we had a group picture. The last segment of the day was called **Web security** and had three presentations. '**Where is the web still insecure? Regional scans for HTTPS certificates** describes the background, methods they used and shared the repository details as well. **Fake Chatroom Profile:** This was a very hard hitting presentation that started with some real life incidences to illustrate how the predators in chatrooms prey on young teenagers and even children. He then talked about their way to combat it by developing a model to predict age and gender from chat. **Combining threat models with security economics:** Graphical threat modelling, security economics and Raas explanation was covered in this presentation.

20th September Presentations

The session started with a keynote speech called **Developing for the long term** by **Lars Knoll**, CTO of the Qt Company. He talked about the company history and best practices for a development architecture. This was followed by a segment called **Biometrics** that had three presentations. **Accessing face image quality with LSTMs** started with existing solutions, neural network methods that are currently in use and presented the case that machine learning in general and neural networks in particular is the way forward for face quality sensors. **Baseline evaluation of smartphone based finger photo verification system: A preliminary study of technology readiness:** Most systems in practice use the concept of finger prints. But this paper introduces the concept of finger photo taken by a smartphone

camera and using it to validate identity. **Towards fingerprint presentation attack detection based on short wave infrared imaging and spectral signatures** talked about presentation attacks and mentioned that they are the easiest attacks to execute with very little technological knowhow. She mentioned that fingers made from orange PlayDoh are the hardest for machines to identify but fairly trivial for humans to identify. She then talked about the proposed fingerprint PAD method.

The second segment called **Malware** had three presentations. **Fighting ransomware with guided undo** identifies common problems in fighting ransomware and shows show a move to personal cloud storage allows for a paradigm shift in ransomware protection. **Source code patterns of cross site scripting in PHP open source projects** was the second presentation and the segment ended with **comparing open source search engine functionality, efficiency and effectiveness with respect to digital forensic search** which used elastic search and Solr.

It was a very valuable opportunity for me to attend so many great presentations and speak to professors and colleagues about the possibility of future collaboration.