Travel Report of COINS Workshop and NIKT Conference (18-20 Sep 2018)

Ph.D. Research Fellow: Dhanya Therese Jose, UiS
Supervisor: Professor Chunming Rong, IDE, UiS
Co-supervisor: Associate Professor Antorweep Chakravorty, IDE, UiS
Co-supervisor: Professor Martin Gilje Jaatun, IDE, UiS

Introduction

It was a great pleasure to go to Svalbard for the COINS workshop and the NISK conference. Same time it was exciting to attend conference in Svalbard, which is the northern most town in the world. It is rather coincidence that Svalbard has a Global seed vault, for securing seeds from all over the world and we were there to attend the Computer and Information security workshop and NISK. Securing data and human need in same land.

COINS Workshop: 18th September

With great excitement, I attended the COINS workshop as I know that this is a great opportunity for me to learn and understand many things as a new PhD student. Around 13:00 on 18th Sep the COINS workshop started. We got a delightful welcome from **Hanno Langweg** and **Urszula Nowostawska** with the COINS t-shirt and hoodie. After that a quick introduction by the participants and agenda of the workshop. Followed by eleven presentations, out which five from those who have completed PhD, shared their experiences while doing PhD and the life afterwards. Others also presented their current works which was quite informative and useful.

In first session, three presentations were there about the lessons learned from doing a Ph.D. **Chris Carr from NTNU: How to get (and not to get) a PhD + why you should / shouldn't travel**. In this he had two parts, first part was about the work-life balance, research, your supervisor, travel and useful tips for writing the thesis. Second part was about a book called "The lean PhD Approach". The three main approaches are Minimum viable paper, Rapid prototype and oriented to the end-user. **Andrii Shalaginov from NTNU: Ph.D: "Mission Impossible" or "Roadside Picnic"?.** He was also focused on the work balance he should have and then about the lessons he learned during hid PhD journey. The last presentation from that session was the inspiring **Bo Sun from UiB: There is always light at the end of the tunnel.** Her presentation was different from others because all the slides she used were her own photographs. With the photographs she explained about the difficulties she faced during the first phase for her PhD and the good things happened in the second phase.

By 14:40 the technical session started. In that session six PhD students presented their current works. Mentioning some of the knowledge or information I gained from the respective topics. **Adam Szekeres from NTNU: Towards predicting individual human decision making in the context of IoT security**. He explained about the three main task he done, such as CoP & CIRA, CEO profiling with IBM Watson personality insights service and Value prediction from demographic features. **Ali Khodabakhsh from NTNU: Fake Face Detection: A Biometric Approach.** It covered mainly detection methods, biometric and presentation attack detection and detection performance. **Jan William Johnsen from NTNU: Identifying Central Individuals in Organised Criminal Groups and Underground Marketplaces. Mazaher Kianpour from NTNU: Cyber Risk Quantification for Business and Economic Gain.** About Digital Ecosystem and Managing security and insecurity externalities which explains the free rider and first mover advantages. **Muhammad Mudassar Yamin from NTNU: Importance of**

autonomous teams in operation-based cyber security exercises. Table top based cybersecurity exercise and operation-based cybersecurity exercise are the two types of cyber security exercise he mentioned. From this presentation, I got to know about an useful paper for my research as well. **Shukun Tokas, UiO: Language-based mechanisms for GDPR compliance.** Detailed explanation about GDPR policy validation for data collection and the information about SeCreol and PriCreol was quite useful.

Third session after the final break started by 16:15. This session deals with the life after PhD, each means find a job or Startup plans. **Berglind Smaradottir from UiA: Experiences from doing a Phd in ICT at the University of Agder – How to find a job afterwards?** She shared some experiences during her PhD and then about how to search for jobs after PhD. **Bikash Agrawal from UiS: A journey from PhD to Startup.** He shared his experience from PhD to startup and also mentioned about a book called "The lean Startup". It was inspiring.

After all sessions, by voting selected two COINS student representatives. I am really happy about my decision to join COINS. I am looking forward for more COINS events.

NIKT: 19th and 20th September

NIKT is a joint national conference consist of **NIK, NISK, NOKOBIT** and **UDIT.** On 19th Sep the official conference opening done by **Ellen Munthe-Kass**, Head of the department UiO. After that the **UDIT keynote** speech by **Prof. Barbara Wasson**, leder av SLATE about **Learning Analytics: What is it and what is its role in education**. It helps to understand about SLATE, learning analytics, how LA enables adaptive learning systems, roles of learning analytics and some details about their on-going projects. Another **NISK Keynote** was also there on the same day afternoon session by **Elise K Lindeberg**, security director of NKOM.

Three sessions with nine paper presentations in total was there on 19th September. The sessions were named as Crypto-primitives, Crypto-protocols and Web Security.

For Crypto-primitives: **A Successful Subfield Lattice Attack on a Fully Homomorphic Encryption Scheme**: This paper contains NTRU and FHE scheme and FHE scheme´s based binary operations. This scheme requires additional operation KeySwitch and ModSwitch to be fully homomorphic. **Improving the generalized correlation attack against stream ciphers:** The proposed solution for generalized correlation attack are using constrained approximate search and bit -parallel implementation. Third person was not there and he presented after the web security session on the same day. The paper was **Debunking blockchain myths:** He explained about the seven myths7 misunderstanding about blockchain, which are about storage technology, mining, peer to peer, private blockchain, etc. It is refreshing the blockchain topics, as I am working on blockchain.

For Crypto-protocols: **Distributed Personal Password Repository using Secret:** In this mentioned but the existing technical solutions, the concrete protocol, details of pilot experiment conducted and the conclusion that it is practical and very used friendly. **The tension between anonymity and privacy:** Stated with GDPR information and its importance, then move on to sequence of Ad-hoc patches, syntactic or checkable privacy, deterministic sanitizer, counter examples and differential privacy.

Before the last session of that day there was a group photo session. For Web Security: **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:** It was a very relavant topic nowadays and the way he presented it was excellent. He explained about the on-going project named Cyber security project, which having a goal to protect children from sexual abuse in internet. Aim to predict age and gender detection from chat and he updated the current status on their project. **Combining**

threat models with security economics: Graphical Threat modelling, security economics and Raas explaination was informative in this presentation.

Keynote on 20th Sep were NIK keynote **Developing for the long term – Lessons learned through 20 years of Qt by Lars Knoll**, CTO of The Qt Company and NOKOBIT Keynote **Tiden med EDB of fargefjernsyn – før vi ble fanget I nettene by Jørgen Fog and Arild Jansen**. There was also a Special session on **Personal Programming for All by Trygve Reenskaug**.

Two sessions with six paper presentations in total was held there on 20th September. The sessions were named as Biometrics and Malware.

Biometrics: **Assessing face image quality with LSTMs:** It deals with the existing solutions, neutral network methods used and the conclusion made is the machine learning in general and neutral networks in particular is the way forward for face quality assessors. **Baseline Evaluation of Smartphone based Finger-photo Verification System: A Preliminary Study of Technology Readiness:** Instead of finger print finger photo recognition system was introduced in this. **Towards Fingerprint Presentation Attack Detection Based on Short Wave Infrared Imaging and Spectral Signatures:** It was about biometric recognition, attacks and the proposed finger print PAD method.

Malware: **Fighting Ransomware with Guided Undo:** This paper defines general problems fighting ransomware with generic properties. **Source Code Patterns of Cross Site Scripting in PHP Open Source Projects.** And the final paper presentation was **Comparing Open Source Search Engine Functionality, Efficiency and Effectiveness with Respect to Digital Forensic Search:** For this work they mainly used Elastic search and Solr.