REFLECTION REPORT FOR

NISK S2017

Coins has funded my participation for the The Norwegian Information Security Conference, NISK 2017. This year NISK was organized in Oslo, Norway.

I. About NISK

The Norwegian Information Security Conference is a national conference that brings together researchers in IT-security, mainly from national community, but also from the international community.

The rest of this report will present some of the main takeaways of the workshop.

1. Security Management

This session was an opportunity to learn about security related research done by people whose main expertise is another field of social sciences.

For instance, we had a talk from the NUPI institute, who conducted both a theoretical and a field study on the role of cyber security in newly digitalized developing societies, taking Myanmar as a case study.

Myanmar Is a country which has finished its military dictatorship in 2011, and that was the first time citizens got access to the internet and its services. This means that this is a country where cyber security literacy is very low. Furthermore, the government has not laws in place to regulate the use and misuse of the internet. This makes Myanmar an attractive location for hackers to base and route their attacks from, as there is little infrastructure to trace the attacks, and make them accountable for it.

Furthermore, the case of Myanmar is of particular interest to Norway, given that Telenor has become of the two major telecom operators there. This means that Telenor has become a major political actor in a foreign country. Observing how will Telenor deal with the government in relations to its citizens digital transactions will be interesting to observe. On the other hand, Norway is also one of the main foreign donors to Myanmar with programs being set up in place to promote democracy. These two aspects of the Norwegian involvement through its government and industry might be tricky to reconcile of conflicting goals are to ever arise, which is a likely situation to happen.

Siri Bombarner from Mnemonics also presented her work around why it is important to consider the ethical aspects when trying to decide on whether to share thereat intelligence or not. Her talk presented the view of deontologists and consequentialist philosophies on the question.

The talk presented by Siri was a nice complement to the keynote speech held also by a Mnemonic security practitioner, and in which he focus on defining threat intelligence. He then moved into talking about the different levels in which we can analyse, detect, recover and protect from cyber threats.

2. Cryptography

One of the talks that were presented during this sessions focused on analysing the security of the CHACHA protocol against differential and linear attacks. The authors relied on integer based linear analysis in order to experimentally test for lower bounds.

During the same session, Britta hale presented the results of a quantitative study conducted at NTNU. The goal of the surveys was to capture the perception of the secure instant messaging applications within the sampled population.

3. Panel discussion

The panel was composed of security practitioners from both academia and industry, who all shared their experience working in the field of security as well as their view on the topic of security by design.

All the participants stressed the importance of education in making sure that we have developers who not only can write code, but can write code securely.

It was also noted that the GDPR is a very positive step towards moving security to the forefront of things that all companies need to care about if they are to be compliant with the EU rules.

Finally, the panel opened the floor for questions from the audience.

4. *Forensics and Biometrics*

As a result of an ongoing research project between the university of Oslo and NR, the team have access to a wealth of real life data from the university’s traffic over an extended period of time. The specific paper presented in NISK was about using DNS traffic in order to detect potential threats. This study relied on a deep learning techniques, namely convolutional neural networks.