Travel Report for NISK

Xiaojie Zhu

January 2, 2017

1 Outline of the NISK

The Norwegian Information Security Conference(NISK) was organised by the department of computing, mathematics, and physics and the ICT engineering research programme at Bergen University on the 29-30 November 2016.

Except the invited talk, following topics are discussed in the conference.

- Malware detection and coding theory. There are three related papers, "memory access pattern for malware detection", "hey tpm, sign my transaction", and "message passisng decoding for self-dual F4-additive codes"
- Intrusion detection. Compared with above topic, there are only two papers, "constrained row-based bit-parallel search intrusion detection" and "data-driven approach to information sharing using data fusion and machine learning for intrusion detection".
- Cellular and network security. In this topic, paper "security vulnerabilities of cellular communication systems" and " an end-to-end security model of inter-domain communication in network function virtualization" are presented.
- Cryptography and hardware security. This is the last topic for the whole conference and two papers related to hardware's security are presented. They are "on trends in low level exploitation" and " decryption phase in norwegian electronic voting".

2 What i learned and my thinking

In the conference i mainly focus on two presentations. One is the "memory access pattern for malware detection", "hey tpm, sign my transaction". This presentation

tries to address the malware detection by analysing the memory access sequences by a tool provided by Intel Pin. The basic assumption hold by this paper is that opcode n-grams are reliable features and opcodes with similar arguments will produce similar memory activity. Based on the dataset *VirusShare repository*, authors did a experiment and showed that the traditional machining leaning methods, e.g., Native Bayes, Bayesian Network, k-Nearest Neighbours, Artificial Neural Network and Support Vector Machine, can achieve accuracy more than 94 percent under 800 features used. Although it gives very clear description about the experiment results, there are no clear description about the training dataset and test dataset, which is very important to evaluate the approach. Moreover, if they could detail the separation method used for selecting training and test dataset, it will be appreciated.

Another presentation i am interested is "data-driven approach to information sharing using data fusion and machine learning for intrusion detection". This presentation tries to tell us applying machine leaning approaches to event classification is promising. One thing that is very interesting is that their model is built based on both academia and industry. It gives a lot interesting requirements that should be realised in a process model. In addition, they also proposed the mechanism of information sharing in the process model, which is very important in intrusion detection. However, it tends to be ignored by academic researchers. Authors also did a experiment to show the performance. A surprise performance is that only 5 to 9 features are used in the experiment but the accuracy reaches 93.22 percent for k-NN. Compared with above presentation, it is significant to reduce the feature from 800 to 9 with acceptable accuracy reduction. Although this presentation gave amazing experiment results, it did not give clear description how to do the experiment.

Except above two presentations, other presentations and talks are also very interesting. For example, section B, the lecture is still alive, is very attractive, which opens my mind. By attending this conference, i also meet a lot people who have similar interests with me. It provides me a chance to communicate with other researchers about what i am doing and how we can learn from each other.

3 Acknowledgement

I really appreciate Coins for providing me such a valuable chance and i also thank all the presenters for their interesting work and those people discussed with me about the interesting topics. Last but not least, i need to say thank you to all the people who work for this conference. Because of them, we can enjoy the conference.