Reporting participation in NISK 2016 conference

Dmytro Piatkivskyi

December 5, 2016

This is to report my participation in NIKT 2016 conference. The conference took place on November 28 – 30 at Bergen University College, Norway. NIKT is a notable conference that comprises multiple conferences specialized in different areas of information technologies. Apart from specialized conference tracks, there were general topic talks given by invited speakers. The particular interest for me was NISK which stands for Norsk Informasjonssikkerhetskonferanse, that is Norwegian Information Security Conference.

The first presentation of the first day was given by Michael Kölling on developments in educational programming environments. He spoke about difficulties of teaching programming at early stages. To make it easy to understand, programming can be taught in rather playful manner. There is a number of software solutions suggesting block-based visual programming where a student can build simple programs with atomic blocks of code in a drug-and-drop fashion. The block-based programming comes in contrast to traditional text programming. At some point though students have to make the transition from block-based programming to text-based programming. It had been stressed that such a transition makes a major problem not only for students and also for teachers. To attenuate the difficulty of the transition a combination of both can be used.

For getting students more interested in programming and to enable an easy start for them frameworks can be designed. For instance, a graphical tool where a student changes a piece of code and can instantly observe the effect of the change graphically. Some other helpful techniques were discussed to help students better understand code. For example, highlighting different code sections with different colours and indentation. Some education softwares such as BlueJ and Greenfoot were demonstrated.

NISK session A was on malware detection and coding theory. Sergii Banin presented the results of his Master thesis where he attempted malware de-

tection analyzing low-level calls. His approach suggests looking into memory access operation sequences that occur during file execution. While it still allows to detect malware, it destroys classic detection evasion techniques employed by malware designers. The focus of the work was on read and write operations and n-grams they make. Machine learning algorithms performed well in such a setup yielding high detection accuracy up to 98.92%.

Afternoon invited talk was given by Tord Søfteland on testdata in systems with complex infrastructure. The talk started off with a brief introduction of software testing. Tord discussed reusable test data for different test levels - unit, system, system integration and user acceptance tests. The great challenge when it comes to reusable test data is to be realistic enough while not having associations to the real-word entities. One way to deal with the problem is to use real-worl data that has undergone a set of disassociating technique. The choice of many such techniques poses a trade off between security and computational load.

At session C Slobodan Petrovic presented a paper on intrusion detection. Most intrusion detection and malware protection systems are signature-based. It means they detect suspicious activities based on precise description of their content. For that, exhaustive databases have to be maintained and continuously updated with signatures of every known malware. Nevertheless, an attacker can easily avoid detection by changing not important parts of malware. To be able also to detect such changed malware an approximate search techniques may be employed. The price to pay is computational overhead and increased false positives rate. Slobodan Petrovic presented a method, row-based bit-parallel search, that allows extremely fast parallel processing of the search string, thus downgrading significantly performance overhead.

The second day started with a talk given by Leif Nielsen. He talked about history of cryptology, focusing massively on Enigma machine. The cryptoanalysis of the Enigma stared with Polish special-purpose machine called bomba, bomb in English. Alan Turing has built on the Polish machine that allowed him to break Enigma. With the machine an enciphered message could be broken in 20 minutes. 200 such machines were built resulting in 600 messages an hour of deciphering capabilities. Leif finished the lecture talking about the father of the first computer in Norway, Ernst Selmer.

There were also two NISK sessions. Session D was on cellular and network security, while Session E was about cryptography and hardware security. During session D Vasileios Gkioulos discussed the inevitable mistakes made and to be made in cellular communication systems design.

The overall impression was very positive. The talks were interesting and relevant.