# NISK 2015 conference - reflection report

report by Andrii Shalaginov for COINS @ HiG
andrii.shalaginov@hig.no

December 1, 2015

This report reflects given presentations on the 8th Norwegian Information Security Conference (NISK 2015). This year NISK 2015 took place in Ålesund on 23 - 25 November 2015 and was organized by Ålesund University College. It will be presented two days of the conferences and content of each contribution.

## 1 Day 1

The first presentation was *"A New Standards of Ukraine: The Kupyna Hash Function and The Kalyna Block Cipher"* by Oleksandr Kazymyrov who described new cryptographic standards in Ukraine from 2014. Block-cipher "Kalyna" brings new insight into the cryptographically strong standard in Ukraine cause it from before the outdated soviet GOST cryptographic standard was in use. The new block cypher was selected during the Ukrainian National Public Cryptography Competition (200-72010). "Kalyna" provides SPN-based Rijndael-like structure with key length 128, 256, 512 bits. Software implementation of the cypher gave better performance than AES on 64-bit general purpose computer such that Mac Book or similar. Another contribution was a hash function "Kupyna", which is a new Ukrainian standard DSTU 7564:2014 brought into life in 2015 instead on Russian hash function standard GOST R 34.11-94. The authors presented that the hash code can be from length of 8 to 512 bit, though the recommended are Kupyna-256, Kupyna-384 and Kupyna-512. Also 64-bit implementations provides high performance.

The last contribution this day was *"Approximate search with constraints on indels with application in SPAM filtering"* by Ambika Shrestha Chitrakar. Authors presented how the edit distance with constraints can be used in the SPAM filtering. In particular, the Sankoff-Indels and CRBP-indels search algorithms were implemented and search speed was given with respect to the number of search patterns in the database. In fact, Sankoff-Indels is much slower than CRBP-indels and, for example, only on 15 patterns it delays up to 0.5 seconds.

## 2 Day 2

Juan J. Guelfo from Encripto AS[1] was invited as a keynote speaker to give a talk on penetration testing. Juan sketched the main problems with information security as related to the absence of talent and inability to process large scale data manually. Additionally to this, majority of the people came to the area of Information Security due to the large interest and their knowledge can not be considered as highly-technical. Therefore, automated testing is required to meet all necessary security requirements and avoid human factor to be blamed as a week chain. Another aspect that matters in the penetration testing is a value and a level of used expertise since depth of analysis is more crucial for a company than a breadth. This is motivated by

[1] `https://www.encripto.no/nb/hjem/`

application of different passive protection mechanisms that eliminate majority of the low-cost attacks, yet may give a way to more sophisticated one. So, to measure effect from attack on the critical infrastructure "Red Team" requires creative and advanced preparation process to gain all the offensive capability. Additionally to this human factor inside the company is evaluated with Social Engineering. Yet according to Juan this has a relative value, cause if the testing is announced, then no point of doing so, since everybody knows about it.

$2^{nd}$ session of the NISK conference was devoted to education and training in security. *"E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures"* was presented by Aparna Vegendla. In this paper, authors presented different attacks, including attack tree on the e-exam systems. Further, Juan presented more technical work done by him in the contribution *"Improving Computer Network Defence Analysis Training with Adversary Replication Techniques"*. One of the methods to improve network defence is to use adversary replication over the company's networks. Juan gave insight into the tools used at Encripto AS[2]: *maligno* is a open source penetration testing tools written in Python and using Metasploit payloads. It allows to simulate client-server C&C communications; *pcapteller*[3] is a tool for replaying and customizing of previously captured network traffic.

Next contribution was *"Play2Prepare: A Board Game Supporting IT Security Preparedness Exercises for Industrial Control Organizations"* and provided with information regarding the preparedness exercises for social manipulation, zero-day attacks, threats from internet and media. One of the parts was so-called pandemic games that simulate spread of the viruses. Authors performed studies and also got relevant feedback from industry.

The last paper in the session "An Initial Insight Into InfoSec Risk Management Practices" was by Gaute Wangen where he explained in details Information Security Risk Management Practices. This was based on early research from Gaute published in NISK 2013. Though now the extensive survey of about 50 professionals from the area was performed with respect to different factors such that size of the company.

Last session started with presentation *"A STRIDE-Based Threat Model for Telehealth Systems"* by Mohamed Abomhara, who presented a STRIDE[4] threat model by Microsoft and its application in telehealth systems. In particular, Mohamed described thrust levels of system users in health care systems and corresponding components: point-of-care, his infrastructure, health & care sources. STRIDE stands for spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege.

Ian Sutherland from Noroff gave a presentation *"Visualising the Impact of Network Attacks on Business Processes using the DEViSE Framework"* describing the visualization of network attacks, which is a crucial issues due to disruption of services and complex interconnections. Though traditional methods focus on ip, mac addresses, ids logs, system logs, it is still not enough. DEViSE framework developed back in 2004 and helps to modelling the business activity and to use Business Process Model and Notation (BPMN).

The last session was concluded with the presentation *"Enabling Dynamic Security Policy Evaluation for Service-Oriented Architectures in Tactical Networks"* by Vasileios Gkioulos as a part of the TACTICS project. Vasileios first presented the nature of warfare as continuously changing and highly-constrained by ad-hoc networks. Therefore, one way to mitigate the challenges in policies construction is to use OWL-DL semantic ontologies to makes a formal representation of security. The advantage of OWL-DL for Service-Oriented Architecture (SOA) is distributed design, highly scalable, sufficient expressive power, support of flexible implementations.

[2] `https://www.encripto.no/nb/downloads/tools/`

[3] `https://www.encripto.no/nb/2015/08/pcapteller-customizing-and-replaying-network-traffic/`

[4] `https://msdn.microsoft.com/en-us/library/ee823878%28v=cs.20%29.aspx`