Reporting participation in ESORICS 2017 conference

Dmytro Piatkivskyi

September 29, 2017

This is to report my participation in ESORICS 2017 conference. The conference took place on September, 11-15 in Oslo, Norway. ESORICS is a notable conference in the area of information security. The conference consisted of two conference tracks (first three days) and a number of workshops (last two days). The author of the report have attend the main two tracks of the conference and International Workshop on Cryptocurrencies and Blockchain Technology (CBT workshop). COINS has kindly sponsored my participation in the conference.

The two conference tracks consisted of thematic sessions ranging form threat analysis to cryptographic applications. Every morning of the first three days was starting with a keynote speech. The first keynote speech titled "Justifying Security Measures" stressed an important point not only in the area of information security, but research philosophy in general. The message was to clearly state all underlying assumptions used in research reasoning. Often, not considering an assumption, or misjudging it might lead to incorrect interpretation of the whole meaning. The message was mentioned and discussed intensively throughout the conference and found general acceptance.

My personal interest at the conference was Blockchain and social networks session. I was hoping to hear much of relevant to my research. It didn't happen, unfortunately. The last talk of the session was on social networks and had nothing to do with blockchain technologies. The other two talks were quite interesting, but pertained the same narrow-fielded topic - an alternative (to Bitcoin) cryptocurrency, Monero. The first talk title "A Traceability Analysis of Monero's Blockchain" demonstrated how Monero's anonymity property is not perfect. The system suggests masking a user's input in a transaction by including other random inputs into it, but not spending them. Naturally, the eventual anonymity depends on how well the users are choosing

noise inputs for a transaction. Besides, the "owners" of the included noise inputs can claim not participating in the transaction. The paper does not discover new risks in the system, but quantifies the known ones.

The other Monero paper "RingCT 2.0: A Compact Linkable Ring Signature Based Protocol for Blockchain Cryptocurrency Monero" was on the principle building block of the system with allows including noise inputs in a transaction, yet still proving its validity. It is possible thanks to ring signatures that allow to authorize an input among a group of inputs, not disclosing which one is being authorized. One of the authors of the paper, Joseph K. Liu, is the designer of the initial linkable ring signature technique that is used in Monero. He has no attribution to Monero and, in fact, did not know about the existence of the cryptocurrecy, nor did he know about the fact that his invention was used in it. Upon discovery of Monero, he thought of an improvement of his own invention so it suits the needs of Monero better. The improvement is compacting the signatures, so Monero transactions are smaller, hence cheaper. An interesting fact to notice is that Monero price has been driven up considerably following the publication of the paper.

What I missed at the Blockchain and social networks session of the main track was completely satisfied by the CBT workshop. The workshop lasted the whole day and covered many interesting aspects of the becoming ever popular distributed ledger technology. The following topics were discussed: consensus algorithms, mining, networking, payment channels, smart contracts and others. A little disappointment was to see that the research effort is being spread around the core technology, but not much effort is being made to improve the technology itself, or to overcome its most glaring challenges. For example, very little attention was brought to scalability issues. Instead, a ticketing solution was proposed on blockchain, which does not bring any value in my opinion.

A talk I liked particularly was a presentation of Graphene, a protocol for a compact block propagation. The authors used Bloom filters to transfer compactly information about what transactions were mined in a recently mined block. Such solution is intended to minimize the information that is being propagated in the network. Another interesting talk presented an algorithm to find paths in payment channel networks accounting for possibility of splitting a payment into multiple payments.

Overall, I am happy to attend a top-level conference in information security, where I found a proper dedication to the topic of my own research. For which I am thankful to COINS.