MASARYKOVA
UNIVERZITA

Annex No. 11 to the MU Directive on Habilitation Procedures and Professor Appointment Procedures

Habilitation Thesis Reviewer's Report

Masaryk University

Faculty	Faculty of Informatics
Procedure field	Informatics
Applicant	RNDr. Petr Švenda, Ph.D.
Applicant's home unit, institution	Faculty informatics, Masaryk University
Habilitation thesis	Examining and exploiting randomness for cryptography
Reviewer	**Prof. Ross Anderson**
Reviewer's home unit, institution	Computer Laboratory, University of Cambridge, UK

This habilitation thesis tackles the problem of how we test random number generators and clean up their output for use in cryptography. All real-world random sources are dirty to some extent, including those where the noise is quantum-mechanical in origin (ranging from the shot noise used years ago to the quantum optics fashionable recently). How can the intrinsic randomness be measured and distilled?

This problem goes back a long way, and the standard reference has changed over the years from Friedman's index of coincidence to Golomb's test to the NIST test suite. What's next?

Petr comes up first with adaptive tests that try to find circuits or Boolean functions that will compress the sample. These are similar in principle to the low-density parity checks discussed in Fast Software Encryption workshops in the early to mid 1990s and which can be used not just for decoding but for stream cipher cryptanalysis. Using them to test randomness is a neat adaptation; they were tried out on eStream and SHA3 candidates but didn't achieve much.

Much more productive was his work on weak RSA keys, on which there's also a fairly long literature. His contribution here is to work out how to fingerprint keys to their libraries of origin – quite surprising given the 40 years of research and the high level of awareness of the need to generate keys carefully. This was accepted at a top conference (Usenix Security 2016) and led to actual attacks on an Infineon implementation, breaking some TPMs, and also a Yubikey token and an unidentified SCADA system. This attack paper was accepted at another top conference (CCS 17). This is his top-cited paper, with 44 citations at the time of writing.

The third theme concerns extensions of his PhD thesis work on security protocols for wireless sensor networks and whether local compromise can be mitigated using secrecy amplification techniques. This work looks at more realistic threat models for sensor networks, and provides his next three most cited papers.

He has a further top conference paper in “A touch of evil”, also at CCS 17, which looks at how one can use threshold cryptography to make a highly secure HSM out of an ensemble of less secure ones. This is again a line of research that goes back some years (Mike Reiter’s Rampart and Omega systems introduced the model in the early 1990s) and it is a shame that Petr’s paper has failed to get much cut-through, with only a dozen citations. However, now that smartcards can be physically compromised using scanning electron microscopes and HSMs are becoming less dependable as they migrate to the cloud, this may be a promising line of research.

His future research directions include continuing large-scale analysis of crypto software libraries, a topic of growing interest as people think not just about side channels but also about usability from the viewpoint of programmers; and work on multiparty computation.

Overall, Dr Švenda has established himself for several years now as a productive researcher who repeatedly comes up with papers that are on topics other than his thesis topic and that are accepted at first-rate conferences. Some of these papers (in particular the Coppersmith attack paper) have had real impact and came to my attention before I was asked to consider this thesis. There is therefore no doubt that the candidate meets the standard for habilitation.

Reviewer's questions for the habilitation thesis defence (number of questions up to the reviewer)

1. How realistic is the Myst threat model in the modern world? If all 100 of your HSMs are virtual devices on AWS or some other hyperscale system, and that gets compromised, threshold crypto doesn’t help much; the same holds if a buffer overflow is discovered in an HSM or a new power-analysis attack against a smartcard.

2. What’s involved in building systems like Myst out of heterogeneous components?

3. What would an international standard for threshold crypto devices look like?

Conclusion

The habilitation thesis entitled “*Examining and exploiting randomness for cryptography*” by Petr Švenda ***fulfils*** the requirements expected of a habilitation thesis in the field of Informatics.

In Cambridge on March 28 2019

[redacted]