

## **Annex 6: Habilitation thesis reader's report**

### **Masaryk University**

**Faculty** MU Faculty of Informatics

**Field of Habilitation** Informatics

**Applicant** Ing. Pavel Čeleda, Ph.D.

**Affiliation** Masaryk University, Institute of Computer Science

**Habilitation Thesis** „Network Traffic Analysis for Cyber Security“

**Reader** Dr. Theo Tryfonas

**Affiliation** University of Bristol, United Kingdom

### **Report Text (as large as the reader deems necessary)**

The report aggregates the findings of original and novel research in the domain of network intrusion detection and puts forward a number of ideas for the improvement of security management in the context of computer networks. The candidate has published extensively to appropriate peer-reviewed venues of good international standing, having had significant contribution to the papers included in the habilitation thesis. He demonstrates advanced knowledge and competence in a number of relevant fields, including network flow analysis, malware analysis, hardware-based intrusion detection, computer emergency response procedures and technologies etc.

Evidence of successful research goal setting, understanding of current research challenges, awareness of the state-of-art as well as implementing and evaluating research ideas, are provided throughout. For example the candidate's work in the analysis of botnets ('Chuck Norris') and the related experiences led to a research project idea ('CPG'), which demonstrates how the candidate is able to develop research programmes independently, through understanding of current challenges. The candidate has also identified the significance of a number of key emerging areas such as security of embedded and proprietary systems and protocols (e.g. BACnet), which I believe represent opportunities for research growth and may provide ample opportunity to the candidate for further work.

In terms of future work and growth of ideas, I would encourage the candidate to consider submitting mature pieces to the venues of the highest calibre, including conferences such as RAID and USENIX. These are venues that are absent from the portfolio presented, however given the current early stage of the candidate's academic career, this is understandable. In any case, I am particularly impressed by the candidate's perceived contribution to research results exploitation, through a company that span out of European R&D activities. This gives me the confidence that the candidate considers his work in the context of its application and is able to participate successfully to commercialisation plans, as they may be required by funders such as the European Union and national councils.

Finally, based on the work presented, I am overall confident that the candidate is someone with the required qualities for the fulfilment of an academic post and in particular that he demonstrates the ability to generate ideas for and supervise research programmes – both essential skills of a research supervisor of PhD students.

**Reader's questions to answer to defend the habilitation thesis (number of questions is upon reader's consideration)**


1. The candidate rightly identifies the 'looser' nature of security requirements in academic and ISP related networks and the management flexibility that these infrastructures demand. In my experience, the traffic profiles of campus-wide networks are subject to change because of the impact of wireless connectivity (e.g. eduroam) and BYOD practices. I was wondering what potential implications are there for the monitoring of traffic flows and how easily would the proposed approaches be adjusted to suit these, esp. when hardware-assisted?

**Conclusion**

Pavel Čeleda's habilitation thesis of "*Network Traffic Analysis for Cyber Security*" *does* meet the standard requirements for a habilitation thesis in the field of Informatics.

In...Bristol...on ...31/03/2014.....

Dr. Theo Tryfonas

 (signature)