M U N I

Annex No. 10 to the MU Directive on Habilitation Procedures and Professor Appointment Procedures

HABILITATION THESIS REVIEWER'S REPORT

Masaryk University	
Applicant	RNDr. Jan Vykopal, Ph.D.
Habilitation thesis	*Teaching Cybersecurity Hands-on*
Reviewer	**Prof. Fabio Massacci**
Reviewer's home unit, institution	Department of Information Engineering and Computer Science, University of Trento, Italy

It has been a pleasure for me to read dr Vykopal's habilitation thesis as I found the work comprehensive, coherent, and innovative. It is also extremely relevant in terms of impact given the current skill gap in Europe on Cybersecurity, a high priority of all European Union states.

The gist of the contribution of this habilitation is to develop methods for hands-on technical cybersecurity training that are both effective and efficient.

The systematic literature review well describe the literature on the field and provide evidence on the current limits of the field.

The development of the KYPO framework was also interesting and challenging. I particularly appreciated the fact that **individual sandboxes have a network structure** of their own. Typically CTFs competitions are run with the individual sandbox is one VM and a full mesh of all-against-all. This flat structure convenient for the organizers but lack realism. Instead KYPO could address this type of realism. As far as I know only DeterLab at the ISI in the USA is able to provide a similar infrastructure among the academic domain.

I also found very interesting the development of a **hybrid architecture for cyber training with industrial control systems**. There are only an handful of such benchmark that students can use (this is an important distinction): one in Bristol and one in Singapore.

The development of **mechanism for short feedback loops** is also a very welcomed innovation in particular for complicated games such as CTF where the pure "success or failure" scores and the number of the flags do not make justice to the complexity of the learning activity.

In terms of **publications** the work has been accepted at several relevant, high impact conference in computer science education (most notably IEEE FIE and ACM SIGCSE) and a respected journal in the domain (Computers & Security). This is a solid proof that the work of the author is scientifically recognized in the community.

After reading the habilition I ended up thinking "uhm, I should use these infrastructures myself." I already pointed the papers to some of my collaborators and started thing to whether I could ask Jan to actually use it for my classes. This is in my opinion the strongest proof that dr Vykopal's work is outstanding.

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

1) It is a pity that the commentary does not discuss the position of the authors in the field. So focussing on Figure 2.3 in the full thesis, where does the author seem himself most contributing his top 3 choices?
2) Which technical feature of the KYPO system would actually contribute most to the above answer?
3) What type of attacks actually distinguishes the use of a purely virtual Cloud Testbed and an ICS testbed. Can we quantify such a difference in terms of learning objectives?
4) How many exercises actually fully exploited the capability of the KYPO framework for networked domains? How complicated were such domains?
5) With the reference to the question above, I would like to know if there is any difference in the achievement of learning objectives on cybersecurity capabilities by students running attack scenarios in more complicated networks. In other
6) In summative assessments how to distinguish the evaluation of the individual from the evaluation of the group? This seems a key aspects and it is a bit glossed over in both the commentary and in the papers.
7) I do not agree that the network logs are representative of a normal situation and therefore researchers can use them to test what happens. The number of attacks present is disproportionate as well as the effort that defenders can dedicate to find attackers. In reality defenders have to spend more time updating their systems. I would like some comments on how to make it more realistic.

Conclusion

The habilitation thesis entitled "*Teaching Cybersecurity Hands-on*" by RNDr. Jan Vykopal, Ph.D., **fulfils** the requirements expected of a habilitation thesis in the field of Informatics.

Date: 18/Aug/2023 Signature: