MUNI

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. Roland van Rijswijk-Deij**
Reviewer's home unit, institution	Faculty of Electrical Engineering, Mathematics and Computer Science, University of Twente, The Netherlands

I have read Dr. Vykopal's habilitation thesis with great interest. As Dr. Vykopal writes, with society's dependence on information technology, it is vital that we train the experts to protect our civil society against threats by both cybercriminals and nation state actors (as cyberwarfare conducted by actors related to the Russian regime demonstrates). At the same time, I echo Dr. Vykopal's remark that the number of trained cybersecurity professionals at all levels of post-secondary education is far below the needs of society. This makes the topic of Dr. Vykopal's habilitation thesis highly relevant for our modern-day society: teaching cybersecurity skills.

I greatly appreciate that Dr. Vykopal takes a hands-on approach to teaching cybersecurity skills. In my view, the work in the thesis bridges the gap between common training methods in the field (CTF, CDX, table-top exercises, ...) and sound educational practices (measurable learning goals, comprehensive student assessment, ...). The works discussed in the thesis advance the state-of-the-art by making new tools available to teaching professionals that teach cybersecurity skills and by providing empirical evidence that these practices actually work. A systematisation of hands-on cybersecurity teaching is direly needed, as without this, we risk compromising the quality of cybersecurity education. I believe Dr. Vykopal's work provides a starting point for maturing the discipline of teaching cybersecurity skills.

I value the comprehensive overview of training methods that Dr. Vykopal provides in chapter 2 of the commentary. Many of these training methods are commonplace in the professional cybersecurity workplace, but they are slow to make their way into academic teaching. It is easy for academics to dismiss these training methods as "too practical" (as it allows them to stay in their comfort zone of classical teaching). I believe, however, that this is a missed opportunity: the cybersecurity professionals we train at bachelor and master level will almost all go into industry, where these types of training and skills are direly needed. I therefore applaud Dr. Vykopal's efforts in taking training types like CTFs and CDXs and giving them a solid grounding in academic education. I firmly agree with Dr. Vykopal that a strong hands-on component in teaching is the best way to equip students with the skills they will need in their professional lives. One worry, however, remains in my view: developing and maintaining materials for the types of hands-on training Dr. Vykopal discusses is highly labour-intensive. While Dr. Vykopal has made promising steps to automating some of the tasks involved in this, he notes in his conclusions that further automation is left to future work. I would be interested to hear his thoughts on how this could proceed in the future.

The KYPO CRP that Dr. Vykopal has put together with colleagues is a very valuable contribution to the state of the art. In my view, this type of open tooling and courseware can be part of the solution to the challenge of developing and maintaining training materials. I see potential for the development of a community around such a platform in which education professionals can share exercises or even entire courses that build on a common toolset. In that light, Dr. Vykopal's collaborations with universities in Singapore and the US are a promising start. At the same time, a platform that is as complex as KYPO comes with its own maintenance challenges. It is a large open-source project. I commend Dr. Vykopal and team for maintaining this for such a long time. I looked through the online repository and note that the contributions to the project seem to come mostly from the project team. I am curious as to the future direction this project will take: are there plans to more actively build a community of contributors to the actual platform and/or are there plans to build a community of practice around it?

The idea of the adaptive training module that Dr. Vykopal developed and integrated in KYPO CRP is interesting. It can alleviate the tasks of teachers or teaching assistants when training large groups of students by offering a more flexible learning path. Introducing this practice, which is already common in other fields, in the cybersecurity environment is highly valuable, given the need to graduate more cybersecurity professionals. One thing that is not discussed in the commentary or the paper about this system is how the selection of tasks maps to learning goals. As an instructor, I would typically set learning goals I expect students to achieve during a course, and I would map those to modes of instruction in the course. Perhaps this is interesting future work, to create a stronger link to learning goals such that an analysis of the learning path can also give instructors a feeling for the extent to which students have mastered the materials. I can even imagine a controlled study in which the extent to which the taken learning path in the automated environment corresponds to success or failure on final exams or tests.

Finally, I note that the work in this habilitation thesis focuses almost exclusively on (highly) technical cybersecurity skills. Seen from the point of view of the computer science discipline, this makes sense. As Dr. Vykopal remarks in his conclusions, however, cybersecurity extends well beyond the realm of technology and also has strong psychosocial, economic and policy aspects. To address these other needs, I would encourage creation of an educational agenda to extend the approach outlined in the habilitation thesis to (some of) these realms. A suggested starting point for this would be to collaborate with researchers from behavioural sciences to assess the behaviour of cybersecurity students and professionals as they perform hands-on training (e.g., CTF challenges or extensive multi-day CDX challenges).

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

I wrote down all of my questions, but I would not expect all of them to be answered (depending on the time available for the defence).

- In Section 2.1, you give an overview of the state of the art in cybersecurity education and list various immersive (CTF, CDX, ...) and more offline (but also more cost effective) approaches such as table top exercises. For both categories of work, my question would be: what is the longevity of exercise materials? In other words: how long can exercise materials be used before they become outdated (because, e.g., attacks or defences have moved on)? Especially for the latter category (offline, table top, ...), it seems to me that part of the cost savings hinges on re-use, but to what extent is such re-use feasible?
- In Section 2.3, you discuss your contributions. Regarding one such contribution, you note that papers on cybersecurity education of talk about "[practices] in the context of a North American university.". My question would be: what would be different in Europe (or if you want to be even more specific, Czechia)?
- In Section 2.3, you discuss a contribution on the analysis of CTF games. You note that there is "[room for covering other topics] such as human aspects of cybersecurity". I fully agree with you, and my question would be: what are ways to do this?
- In Chapter 4, you discuss various instructional methods and discuss their benefits and challenges from both the student/learner and the teaching perspective. For the category of "Serious Games", you list as one of the teaching challenges that "Students underestimate the complexity of the project". I wonder if this also implies that teachers underestimate how hard it is for students and what could be done to improve the method to make it more accessible (and whether, in your opinion, there is a need to do so, or not).
- I really enjoyed reading about the adaptive training approach in Chapter 4; one question I am left with after reading the chapter and the paper is: how interdependent are training tasks (i.e. if a student does one task at one level, do they then have to stay at that level)? And a follow up question would be: how well does performance in phases 1..n then predict the required difficulty level for phase n+1? Finally, for this approach, I wonder if there is a risk for students to underperform by gaming the system such that they get assigned the "easier" tasks, and if so, what could be done to prevent this?
- In your conclusions, you discuss that your contributions mainly address teaching technical aspects of cybersecurity, but you also remark that "[you] believe that tools and principles used for training technical skills can be adopted [in the context of training of] communication and decision-making skills". I fully agree that such training is needed, beyond believing your tools and principles can be applied, *how* would you apply them? Can you sketch and example?
- In your conclusions, you remark that preparing course materials and exercises is a time-consuming task. One worry I have is about the longevity of such materials; cybersecurity is a rapidly evolving discipline, and I worry that this year's materials might already be outdated next year. How could we distil a more abstract skillset that we can capture in materials that stand the test of time a bit more? How could this alleviate the task of training cybersecurity professionals such that we can train more of them?

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:
August 17th, 2023

Signature: