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	Raimundas Matulevičius, PhD., Prof.
Reviewer's home unit, institution	Institute of Computer Science, Faculty of Science and Technology, University of Tartu

Jan Vykopal has delivered the thesis on "Teaching Cybersecurity Hands-on" for a habilitation degree at Masaryk University. This document contains my review of the habilitation thesis. Ultimately, I conclude whether this thesis is acceptable for the habilitation degree.

The thesis comprises a complementary and collection of 14 articles published in international venues. The complementary consists of 88 pages, including 5 chapters (1. Introduction, 2. State of the Art, 3. Training Environment, 4. Instructional Methods, 5. Conclusions, and Bibliography). The bibliography has 105 references.

In the introductory chapter, the candidate provides the work motivation and highlights the need to explain what, why, and how to teach cybersecurity-related topics to ensure the high-level competencies of the trainees. The work considers three research questions: one on how to create and adopt the cybersecurity teaching environment; second on the methods suitable to teach cybersecurity hands-on; and third on how to conduct cybersecurity training efficiently. Although the introduction misses the overview of the research and exploration approaches used in this thesis, the introduction explicitly defines how these research questions are answered in the subsequent chapters of the complementary.

In the second chapter on state-of-the-art, the candidate first describes the instructional methods, including the hands-on labs, competitions and games, defence and offence exercises, and unplugged-based teaching approaches. Secondly, the candidate situates his research in cybersecurity education, which is a part of the computing education research field. The leading candidate's contribution to the state of the art is the systematic reviews of the themes and topics, skills and knowledge taught in cybersecurity, and data mining and learning analytics to obtain knowledge from the data collected during cybersecurity training exercises.

The third section is dedicated to the training environments, whose main components are training tasks (delivery methods), sandboxes, and learning analytics. The training environment is used by the trainees/students and by instructors/teachers. The candidate describes two cases in the thesis: the scalable virtual and cyber-physical learning environments. An example of a scalable virtual learning environment is the KYPO Cyber Range Platform. The industrial control systems (ICS) testbed is an instance of the cyber-physical learning environment. The primary candidate's contribution, reported in this chapter, includes the teaching experience gained while teaching 650 students in 38 training sessions using the KYPO Cyber Range Platform. Also, the candidate says on the lessons learnt from the 13-week course teaching using the ICS testbed. In both cases, the candidate focuses much on describing the technical

and managerial usage of the environments but does not consider how the learning objectives are achieved and whether the trainees obtained the skills and competencies in cybersecurity.

The fourth chapter is dedicated to instructional methods. The candidate focuses on cybersecurity exercises, serious games, and efficient learning. Complex *cybersecurity exercises* involve different roles (red, blue, green, and white teams) and must be carefully planned; providing timely and valuable feedback to the exercise participants becomes essential. The candidate reports on the experience of. Using the CDX scoring system indicates that the learners value the received feedback, although they lack some details about particular aspects. Another contribution of the candidate is the collection of network traffic traces, data gathered from the CDX logs. Developing and testing *serious games* is an exciting teaching and learning approach that contributes to students' different technical, management and transversal skills. The candidate discusses how the automated means – the APG toolset – can help detect suspicious student submissions.

In the section on *efficient learning*, the candidate illustrates how data about interactions between the learners and the learning environment can contribute to the efficiency of the teaching. Firstly, the training format and the tutor model are presented. These can be incorporated into the KYPO Cyber Range Platform. A case study involving 114 graduate and undergraduate students from high schools and universities, on the one hand, illustrated that an efficient learning approach is suitable for the majority of the students, who remain motivated to complete the given tasks. On the other hand, the case study illustrated that such exercises require intensive instructors' involvement. Thirdly, additional features, such as visual analytics, feedback, trainee and milestone graphs, and patterns definition, are essential characteristics contributing to the efficiency and analysis of the efficient learning approach.

In the concluding section, the candidate highlights the key achievements focussing on developed training environments, applied methods to achieve cybersecurity skills and competencies, and means to provide student feedback. Although the discussion does not explain how students achieve different learning outcomes and improve their skills using various instructional methods (whether the skills and competencies are acquired), the primary author's contributions are thoroughly defined and tested in empirical settings. All case study presentations could benefit from describing the validity threats and the means to mitigate them.

Fourteen selected international peer-reviewed publications (five journal articles and nine conference papers) have been included in this report. A group of researchers co-authors all publications, but the habilitation thesis explicitly indicates how much the candidate contributed to the preparation and writing of these publications.

The first three publications contribute to the state of the art. In the article "*What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences*", the authors elicit the technical and social aspects of cyber security teaching using the systematic literature approach. Another article on "*Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges*" highlighted that teaching the technical aspects of cybersecurity is preferred against social concerns. In the article "*Applications of Educational Data Mining and Learning Analytics on Data From Cybersecurity Training*", the authors perform a systematic literature study to explore the impact of educational data mining and data analytics in cybersecurity teaching.

The other three publications discuss the architectures and features of the learning environments. In the paper "*KYPO Cyber Range: Design and Use Cases*", the authors present a set of use cases to evaluate the KYPO cyber ranges. Elsewhere in "*KYPO-4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems*", the architecture of a simulated industrial environment is discussed and assessed in the experimental settings. In

the "*Scalable Learning Environments for Teaching Cybersecurity Hands-on*" paper, the authors discuss the scalable cybersecurity teaching experience using the KYPO Cyber Range Platform and Cyber Sandbox Creator learning environments.

The remaining eight publications concern instructional teaching methods. In "*Lessons Learned From Complex Hands-on Defence Exercises in a Cyber Range*", the authors report on the experience gained from running the cyber-defence exercises involving participants of different backgrounds. Another paper, "*Timely Feedback in Unstructured Cybersecurity Exercises*", presents an approach to providing the time feedback to the learners. The authors share their experience from the "learning by doing" courses in the paper "*Enhancing Cybersecurity Skills by Creating Serious Games*". Here, the students have designed serious games in cybersecurity and thus were able to gain practical skills and discuss the topics with their classmates.

The conceptual model of visual analytics principles to design, execute and evaluate the cybersecurity training sessions is proposed in the article "*Conceptual Model of Visual Analytics for Hands-on Cybersecurity Training*". In the paper "*Benefits and Pitfalls of Using Capture the Flag Games in University Courses*", the authors discuss the challenges (in tasks of scoring, scaffolding, plagiarism, and learning analytics) when designing the CTF exercises. The challenge of cheating is considered in the paper. "*Preventing Cheating in Hands-on Lab Assignments*", where a system for automated task generation is suggested. In another article, "*Student Assessment in Cybersecurity Training Automated by Pattern Mining and Clustering*", the authors apply data mining and machine learning techniques to cybersecurity training data. The paper illustrates that pattern mining helps determine student behaviours, misconceptions and challenging exercises. Clustering helps determine similarities and differences between students' behaviour to find the solutions. In the article "*Smart Environment for Adaptive Learning of Cybersecurity Skills*", the authors report on the training environment for the adaptive cybersecurity skills training. The reported case study illustrates that it helped students to complete the tasks of their appropriate difficulty.

In conclusion, Jan Vykopal has significantly led and contributed to the field of Cybersecurity Educational research. He has researched and developed learning platforms and proposed various methods and approaches for hands-on cybersecurity teaching. His publication record is solid and well-recognized (h-index = 15 in Scopus and h-index=9 in Web of Science).

I recommend awarding Jan Vykopal the habilitation degree.

Reviewer's questions for the habilitation thesis defence (number of questions up to the reviewer) none

Conclusion

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

Date: 05.09.2023

Signature: