Review of a Doctoral Thesis at FIT BUT

Doctoral thesis (hereinafter referred to as "thesis"), title of the thesis:

Name of the doctoral student (hereinafter referred to as "student"), name and surname:

Kamil Jerabek

Name and institution of the reviewer (full name of the reviewer, full name and country of the institution):

Prof. Dr. Pavel Laskov, University of Liechtenstein, Liechtenstein

---

Please state your opinion on the following aspects of (I) the student's thesis and (II) the student's overall achievements, and (III) state your conclusion (a minimum of approx. 300 characters foreach item below is recommended):

I. Thesis

Appropriateness and relevance

Is the area addressed by the thesis appropriate to the particular scientific discipline of the thesis and does the thesis address relevant problems within the chosen area?

The topic of the thesis is very appropriate. Its work revolves around DoH, the new protocol for IP address resolution, designed and standardized in 2018. The main goal of DoH is to enhance user privacy by hiding IP address resolution requests under the confidentiality and integrity "umbrella" of the HTTPS protocol which has become a de factor standard on the Internet. Academic work on analysis of the DoH protocol is currently rather limited. The thesis is very appropriate for computer network technologies and addresses an important scientific problem.

A summary of the contributions of the thesis

From your point of view, please summarize what the goal of the thesis is, what the main contributions of the thesis are, and whether the thesis has achieved the chosen goal.

The overarching goal of the thesis is to develop novel techniques for detection of DoH traffic within HTTPS communication. This goal should be also achievable without development of custom features unsupported by existing monitoring infrastructures - in contrast to several previous works. As intermediate steps, the work has addressed various issues related to analysis of existing DoH infrastructures, benchmark data generation, development of respective detection methods and their experimental assessment.

Please indicate also specific contributions of the student.

Contributions of this thesis are manifold. It begins with experimental analysis of existing DoH servers which sheds light on their important statistical and technical features. Furthermore, the work develops novel methodology for analysis of traffic related to DoH. Based on this methodology, several longitudinal studies are carried out, in order to understand key operational characteristics of DoH. As another important

contribution, several datasets are generated for the task of DoH traffic recognition, and techniques for DoH traffic detection are proposed and evaluated.

Novelty and significance:

Please assess the level of novelty of the results and their significance for the given scientific area, for its further development, and if applicable for possible applications in practice.

The contributions of the thesis are quite novel, especially from the technical viewpoint. Comprehensive studies based on extensive data generation are rare in the field of security and networking. This work a convincing example of how thorough experimental studies can contribute valuable insights, even coupled with simple analytical instruments. The machine learning methodology explored in the last part of the thesis is rather conventional, yet its proper design and implementation constitute a significant contribution in the specific problem field of this work.

Evaluation of the formal aspects of the thesis:

Please evaluate formal qualities of thesis and its language level.

The thesis satisfies, at least in the common understanding of the reviewer, formal requirements for a PhD thesis. It presents several independent scientific contributions which demonstrate significant individual achievements of the applicant. The thesis is well written and easy to follow.

Quality of publications

Has the core of the thesis been published at an appropriate level? Please judge the quantity and quality of the publications. When judging the quality, please take into account internationally recognized standards (WoS/Scopus quartiles, CORE ranks, specific knowledge of flagship publication channels of a given community, etc.) in a way appropriate for the given area of the thesis.

The core of the thesis has been published in several articles appearing in established conferences and workshops (IEEE, ACM). The reviewer is not in the position to formally assess the significance of these outlets in terms of their rankings, yet the overall impression is that the presented work is of solid quality and will be well accepted by the scientific community.

II. Student's overall achievements

Overall R&D activities evaluation:

Does the student's thesis, the results included into it, and possible other scientific achievements listed in the list of scientific activities indicate that he/she is a person with scientific erudition and creative abilities?

The thesis clearly indicates the applicant's high potential for scientific work. It demonstrates his breadth of technical knowledge as well as his capability to identify gaps in scientific knowledge and to close these gaps by developing novel methods and experiments.

Assessment of other characteristics (optional):

More characteristics of the student may be added here (e.g., awards, grant participation, international collaboration, etc.).

III. Conclusion

The conclusion should contain an explicit statement saying whether, in your opinion, the thesis and the student´s achievements until now meet the generally accepted requirements for the award of an academic degree (in accordance with Section 47 of Act No. 111/1998 Coll., on higher education institution).*

* Short overview of both the Act and corresponding internal BUT regulations is enclosed.

The thesis fully meets generally accepted expectations for a PhD research contribution. It addresses a very up-to-date problem, and provides novel and substantial contributions on technical, methodical, and experimental aspects of networking and security. The thesis is very well anchored in existing academic work and provides a critical analysis of its own contributions in light of related work.

Vaduz, 24.04.2024

Prof. Dr. Pavel Laskov