CTU
CZECH TECHNICAL
UNIVERSITY
IN PRAGUE

THESIS REVIEWER'S REPORT

I. IDENTIFICATION DATA

Thesis title:	**Credibility of Encrypted DNS Traffic**
Author's name:	**Bc. Jan Šimůnek**
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Department of Telecommunication Engineering
Thesis reviewer:	doc. Ing. Zdeněk Lokaj, Ph.D.
Reviewer's department:	Faculty of Transportation Sciences (FTS), CTU in Prague

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment **challenging**

How demanding was the assigned project?

The diploma assignment was challenging, student should creatively propose DoH and DoT solution in publicly available DNS resolvers to increase security and confidentiality of the communication. This topic is very important because of rapid increase of electronic communication caused by process digitalization and people paradigm shift.

Fulfilment of assignment **fulfilled**

How well does the thesis fulfil the assigned task? Have the primary goals been achieved? Which assigned tasks have been incompletely covered, and which parts of the thesis are overextended? Justify your answer.

The author fulfilled the assignment with some small gaps in the theoretical part, where the author should write more detailed analysis of security of DNS architecture. On the other hand, the practical part of thesis is very impressive and practically usable.

Methodology **correct**

Comment on the correctness of the approach and/or the solution methods.

The author chooses the right approach to a solution that is systematic based on the theoretical basis and subsequently using the methods.

Technical level **A - excellent.**

Is the thesis technically sound? How well did the student employ expertise in the field of his/her field of study? Does the student explain clearly what he/she has done?

Technically, the work is at a very high level. The work describes in great detail the DNS protocol and its secure variants DNS over TLS and DNS over HTTPS and then implements the analysis of these protocols in terms of security vulnerabilities. I very much appreciate the practical usability of the work, especially the identification of vulnerabilities in the field of DNS protocol family, which is widely used worldwide, and from the point of view of eliminating cyber threats, this is a fundamental finding.

Formal and language level, scope of thesis **A - excellent.**

Are formalisms and notations used properly? Is the thesis organized in a logical way? Is the thesis sufficiently extensive? Is the thesis well-presented? Is the language clear and understandable? Is the English satisfactory?

The structure of the work is comprehensible and clear. The graphic design of the work is good, clear and very impressive.

Selection of sources, citation correctness **Choose an item.**

Does the thesis make adequate reference to earlier work on the topic? Was the selection of sources adequate? Is the student's original work clearly distinguished from earlier work in the field? Do the bibliographic citations meet the standards?

Student has chosen the proper approach of obtaining information, in expected depth. Some of the citations should be listed better.

Additional commentary and evaluation (optional)

Comment on the overall quality of the thesis, its novelty and its impact on the field, its strengths and weaknesses, the utility of the solution that is presented, the theoretical/formal level, the student's skillfulness, etc.

Please insert your comments here.

III. OVERALL EVALUATION, QUESTIONS FOR THE PRESENTATION AND DEFENSE OF THE THESIS, SUGGESTED GRADE

Summarize your opinion on the thesis and explain your final grading. Pose questions that should be answered during the presentation and defense of the student's work.

Technically, the work is at a very high level. The work describes in great detail the DNS protocol and its secure variants DNS over TLS and DNS over HTTPS and then implements the analysis of these protocols in terms of security vulnerabilities. I very much appreciate the practical usability of the work, especially the identification of vulnerabilities in the field of DNS protocol family, which is widely used worldwide, and from the point of view of eliminating cyber threats, this is a fundamental finding. In my opinion the presented diploma thesis has quality much higher than standard of these types of works so there is very difficult to find any mistakes.

Questions:

1) Can you explain potential use of your findings in cyber security tools?
2) Can you describe the typical trajectory of the attack on the identified vulnerability?

The grade that I award for the thesis is **A - excellent.**

doc. Ing. Zdeněk Lokaj, Ph.D.

Date: **16.6.2021**

Signature: