Opponent Review of the Doctoral Thesis

Security Testing in Safety-Critical Networks

(Testování zabezpečení v sítích pro bezpečnostně kritické aplikace)

Ph.D. student: Nils Weiss M. Sc.

Department: Department of Computer Science and Engineering, Faculty of Applied Sciences, University of West Bohemia in Pilsen

Supervisor: Prof. Ing. Václav Matoušek, CSc.
Supervisor-specialist: Prof. Dr. Ing. Jürgen Mottok

Opponent: doc. Ing. Vít Fábera, Ph.D., Faculty of Transportation Sciences, Czech Technical University in Prague

Presented doctoral thesis is relatively extensive, approximately 100 pages of the text and 50 pages of the appendices. The theme is actual, beneficial and suitable for the doctoral thesis. The portion of the software and digital subsystems generally increases in automotive industry and the security (and safety too) is less explored area in automotive than in other spheres (like banking sector). The research in this area is very useful (by reason of some specific in the automotive industry) and automated testing is one of ways.

Firstly, I must highlight a system approach of the Ph.D. student to the problem, very good written text, and also a fact that the output of the work has theoretical and practical parts. The text is divided into 3 sections, the original benefit of the author is in the second and mainly in the third sections. The first part is introductory, it contains an overview of communication buses and interfaces used in automotive industry. The part is brief (how it should be in the doctoral thesis), but summarizes all necessary facts, information about details are referenced to literature.

The second part is focused on methodology and manual security exploration. Vulnerability analysis and its evaluation is partially subjective and "soft-techniques" are usually used. The student is based on existing methodologies and designed own, appropriate, methodology (investigation process) described in four steps. It analyses roles of (ECUs – Electronic Control Units) in cars, then properties of components are identified from the point of vulnerability view (processors, external memories, interfaces) – correctly, these board parts are really places of vulnerability. The measure of vulnerability is described by two scores (impact score and exploitation score), each in the range *low, medium, high*, 1, 2, 3 numerically. The total score is a multiplication product (based on CVSS); the suggested measure is simple and suitable for this purpose. The lack is that the calculation is not described better, e.g. by the equation. Moreover, the author created form template to describe identified vulnerability. I see great potential in use other technique like fuzzy approach in the future to evaluate vulnerability how the student writes in the conclusion.

The student applied his methodology practically – he selected four representatives of boards used in cars, appropriately chosen to cover application areas (gateway, Body Domain Controller, telematics, airbag control). He identified vulnerabilities and he analyzed results in the chapter 5. Very important is that analyze of not only separate vulnerabilities but vulnerability chains is performed. There are dependencies between some vulnerabilities and the "breakdown" of someone opens the way to attack other parts and functionalities of the system.

I have one note to the chapter 5. There is a hypothetical assumption in the chapter 5: „*Assuming that the software update mechanisms would not have security flaws, V8, V13, V17, V20, and V28 would not be present.*" The question is how the assumption is true in the reality. But this assumption helps to understand the impact of vulnerability chains, how the author writes. The conclusion of the chapter 5 is the analysis which targets are suitable for automated testing. Naturally, they are the best interfaces for the author. Regarding the wireless interfaces, the author states: „*The automation capabilities of the entire attack surface Wireless Interfaces have low capabilities for automated vulnerability assessments*". The reason is that there are many variants of communication standards but I think that next research should focus on wireless because these types of interfaces will be in the interest of attention of hackers in the future.

The third part of the thesis is focused on automated testing system design. The student chose diagnostic subsystem with UDS and GMLAN protocol as a target part under test. The core of the tester are an enumerator and scanner which crate transition graph of states of system under test and analyze the graph. The Ph. D. student created necessary theoretical basis (definitions, algorithms descriptions in pseudo-language). The special attention is paid to states into which entry is conditioned by encryption. This part of the graph is described and evaluated extra using statistics (CDF – cumulative distributive function) and he expresses the probability of breaking the cipher. It is the main original benefit of the author – model and algorithm creation and using statistical approach. I only miss better expressed or emphasized relation between transition graph and vulnerability chains.

The benefit is a practical output of the work – testing software. Related to own product, the approach to the design is correct. The author selected free – platform enabling packet analysis and extended it; he described his work in detail in appendix. The architecture is object oriented (according to statement in the text) and it enables easy extension by next enumerators (I suppose in the form of descendant of classes). The software is tested and results are clearly concluded.

The bibliography contains 58 relevant publications. It evident that the student has an overview and he was able to use information from the literature as much as possible. The list of student's publications related to the theme contains 4 items. It is relatively sufficient.

The text is clear, readable and understandable.

Questions:

1. Do you suggest any recommendation to producers how to decrease vulnerability found on your analysis and executed tests?
2. Two of boards contain Linux and QNX operating system. There is some vulnerability due to two bugs. How do you see to use existing operating systems versus proprietary framework?
3. Many vulnerabilities have a physical access to interfaces, external memories (PCB generally) as a necessary assumption. This is not normally possible and it decrease the risk – as you write in your thesis. My next question is related to the "social aspects". It can be misused by technicians in car services or "specially trained thieves" in gangs which can connect to bus for example in night. Do you have any idea to protection?
4. Can you show any structure of your application, for example Class diagram?
5. Do you see any benefit in mapping of your state graph to typical vulnerability chains and following analysis?

Conclusion:

The thesis fulfill requirements for doctoral thesis and I recommend to award Ph.D. degree.

doc. Ing. Vít Fábera, Ph.D.
Department of Applied Informatics in Transportation
Faculty of Transportation Science,
Czech Technical University in Prague
Konviktská 20
110 00 Praha 1

Prague, 2021-10-19

Hochschule
München
University of
Applied Sciences

Hochschule für angewandte
Wissenschaften München

Department of Computer Science
and Mathematics (07)

Prof. Dr.-Ing Martin Hobelsberger
Dean of Academic Affairs
Room R4.029
(0) 89 1265 3779
martin.hobelsberger@hm.edu

cs.hm.edu

Hochschule München · Postfach 200113 · 80001 München

Faculty of Applied Sciences
University of West Bohemia in Pilsen
Univerzitní 2732/8
CZ - 306 14 Plzeň
CZECH REPUBLIC

26.10.2021

Assessment of the Ph.D. Thesis of Nils Weiss, M.Sc. "Security Testing in Safety-Critical Networks ", Assessor: Prof. Dr.-Ing. Martin Hobelsberger

Mr. Weiss focuses in his thesis on the security engineering of automotive systems and components. He explores possible attack scenarios, defines processes to support the analysis of those, develops an open-source tooling for testing components/networks as well as models specific for automotive diagnostic protocols.

The thesis is very well and logically structured into chapters (nine chapters of text and three appendices, bibliography, and list of publications). Motivation of his work and the goals of the thesis (chapter one) are formulated to the point. These goals are tightly connected to the research questions formulated in the thesis exposé and fully support the approach of solving the defined research problem. Goals and research problems have been translated into tasks and objectives which are subject to the chapters two to seven. In chapter eight the results are discussed and concluded in chapter nine. All stated research questions have been answered and subsequent tasks solved.

The presented topic is of utmost actuality and value for the research community and application domain. Throughout his thesis Mr. Weiss provides an excellent summary and review of relevant research to date. Relevant technical background information and introductions to the systems under test are provided in chapter two. This is well written, logically structured and provides the technical setup for the theoretical work in terms of processes and analysis (chapters three and four) as well as the experimental work (chapters five to seven) on security testing. In chapter three an investigation-process as well es descriptions of vulnerabilities are provided. This is done in a structured and formal way which allows for a transfer on future systems and components. The theoretical foundation of this is applied in chapter four and partly chapter five and is followed by a survey on security research. This helps to set the work into perspective to already published related work and strongly supports the approach presented in the thesis. For the benefit of an applicability in real world setups chapter five and six analyze the possibilities and capabilities of automated security testing. For this Mr. Weiss compares existing open-source tools and identifies necessary contributions, needed for an application in pre-defined scenarios. In chapter seven a novel security scanner is introduced. With this Mr. Weiss shows impressively that not only the theoretical foundation was developed and presented but is transferred by him in a tool which could be used by the industry as well as the research community. The most important results from each contribution

chapter of the thesis are summarized and presented in chapter conclusions to connect the contributions together and build a bigger and more thorough picture of the presented problem.

Results and the main contributions of the thesis as

- the development/application of an investigation process for black-box security analysis,
- an Open-Source Framework for (manual/semi-automated) security testing of automotive networks and fully automated security testing of automotive diagnostic protocols,
- an attack-surface model for automotive diagnostic protocols,

are discussed, written clear and understandable, in chapter eight and concluded in chapter nine.

The doctoral thesis written by Mr. Weiss can be evaluated without doubt very positively. The content of the doctoral thesis positively supports the competence of the author to apply and successfully implement the elected theoretical resources. From a formal point of view, the doctoral thesis is very well written, structured and of an appropriate graphical level. Significant parts of the work were already published in world-known journals and/or on significant scientific conferences. The publication list contains five international conference papers between 2017 and 2021. Mr. Weiss is the leading author of four of them. All are published with co-authors. The thesis and the publication list show that Mr. Weiss can perform research independently. Significant parts of the work of Mr. Weiss thesis will certainly be used for future scientific work and provides a very good source for other researchers.

My questions for the Defense of the Thesis would be.

- What would be your take on a methodology (pretending a culture change is possible) for information exchange on security topics between interested parties? Are there best practices on other domains?
- Would an online (in vehicle) security testing solution be feasible? What would be the implications?

Conclusion:
I have reached the conclusion that this work brings several new and novel pieces of knowledge to the scientific community. The core of this work has been correspondingly published. Furthermore, the theoretical foundation of the work can be readily applied by researchers and professionals worldwide using the open-source tools developed by Mr. Weiss. The work can be qualified as a very good doctoral thesis. For this reason, I recommend the acceptance of his thesis for the granting of the academic title Ph.D.

With best regards

Prof. Dr.-Ing. Martin Hobelsberger
Dean of Academic Affairs for the Department of Computer Science and Mathematics

Review of the Ph.D. Thesis

Author: M.Sc. Nils Weiss

Title: Security testing in safety-critical networks

The presented thesis deals with the topic of security testing of safety critical systems in the domain of automotive networks and systems. The selected topic is highly relevant and actual due to the fact that the cars changed from the mechanical machines to the complex distributed computer systems having nearly one hundred electronic control unites (ECUs) interconnected via multiple communication buses and allowing connection to various external communication systems and technologies. The potential hacker attacks are highly probable and the consequences can be fatal.

The presented thesis is divided into several chapters. The first part presents the overview of automotive networks and communication protocols. The second part describes the manual security investigation of the ECUs. The presented methodology defines several standardized attack surfaces and the author also proposed the standardization of the vulnerability scoring system in order to standardize the process and the quantification of the investigation results. Several examples of different ECU investigations are presented. The next part of the thesis deals with the analysis of the identified vulnerabilities and attack surfaces. The author presents analysis of published successful hackers' attacks of the vehicle systems and also the analysis of potentials for attack from the previous chapter. The result of analysis is used for identification of potentials for automation of security testing procedures. The diagnostic protocol is selected as a good potential.

Proposal of the testing automation solution begins with evaluation of existing open-source software frameworks when the Scapy project was selected as a tool for the implementation of the automated testing system. The following part describes the design and implementation of novel automated testing procedure focused on testing of different layers of the diagnostic protocol. This innovative method is based on the definition of the system state diagram and the transitions among the states by use of active automata learning technique to reverse engineer the system behavior. The system allows identification of the most vulnerable states, such as bootloader, system parametrization or hidden OEM specific debugging states. The proper functionality of the presented approach is demonstrated on the successful testing of several different ECUs.

I can conclude that the author reached all the goals, proved deep expertise of the selected domain and presented complex and exhaustive scientific work.

Despite the fact that the presented research is complex and considering many aspects of security of the safety-critical systems, I would recommend to add also the normative. Automotive industry is conservative and a lot of activities and processes are formalized in the standards. Thus I would like to recommend to consider also the standards dealing with the cyber security, automotive system integrity and related. We can name standards like ISO/SAE 21434, GB/T 204-11, ISO 26262 as examples.

I have one additional question. In the thesis the author states that the OEM specific solutions in HW and communication protocol implementations without access of the public to the details of this customized solutions decreases the chance to shift the security of such systems to higher level. That the keeping of these secrets would not stop the organize crime. On the contrary to that the author proposes to present the information publicly in order to increase the security of the system design. Can the author explain his opinion in the deeper detail?

I recommend the thesis to defense.

In Prague, 15thOctober2021

Ing. Aleš Cerman, Ph.D.