Review of the Dissertation Thesis

Thesis title: Model-driven Security Engineering for FPGAs
Author: Ing. Michael Vetter
Supervisor: Doc. Ing. Vlastimil Vavřička, CSc.

The Dissertation thesis deals with the security of FPGA-based designs. The author correctly states that this issue has been neglected, therefore the topic is definitely important and timely. The Thesis proposes a systematic way of determining security threats and a formal way to model them. For this purpose, a novel domain-specific language FPGASECML is introduced. With its help it is possible to model security threats and interaction of different design blocks. Respective implementation and communication rules can be assessed from it.

The Thesis is very well written, with a minimum of typos, it is easy to follow. Honestly, I really enjoyed reading it.

Thesis structure

The Thesis is structured into ten chapters as follows:

- Chapter 1 gives a basic overview of IT-security, FPGA-security, and the motivation and challenges to improve the security of FPGA-based designs. Next, it provides the state-of-the-art in the security of FPGAs. Finally, it presents security gaps in FPGA-based designs and contributions of the Thesis.
- Chapter 2 reviews the security threats and trustworthiness determination, with a focus on FPGA-based designs.
- Chapter 3 summarizes the ways of threat modeling for FPGA-based designs.
- This reasoning then continues in Chapter 4, presenting the system-centric threat modeling and the building blocks needed.
- Chapter 5 then proposes the access restrictions for FPGA-based designs to reduce the threat risks.
- The theoretical analysis is then materialized in the following chapters. Chapter 6 formalizes the security model by proposing a metamodel of a secure FPGA-based design.
- Chapter 7 then proposes FPGASECML, a new domain-specific modeling language to describe the metamodel. From my point of view, the example in this chapter could have been described more thoroughly. Even though the details are not important for understanding the principles, the reader needs not fully capture what the design really does and how does it do it.
- Chapter 8 speaks about validation of structural description of the architecture with respect to security aspects. Again, more details could have been provided directly in the very chapter. When reading it, one must skip between the chapter text and the appendices.
- Chapter 9 proposes using reinforcement learning, particularly the Markov decision process (MPD), to identify further security weaknesses. This is an “icing on the cake” of the thesis. This topic is definitely worth more investigation. Actually, it is worth another Ph.D. thesis.
- Finally, Chapter 10 concludes the thesis by summarizing the achievements.

The text is then accompanied by eight appendices, which are not essential for understanding the most important ideas, but they are needed to understand some details.

It is apparent that the approached problem has been solved systematically, rigorously, modern methods have been used (model checking, reinforcement learning). The outcomes are definitely beneficial, especially the FPGASECML language which filled the gap in the field.

The results were published in two impacted journals, one book chapter, one technical report, and seven workshops. Here I'm just wondering why there are no international conferences. But despite this, I find the publication activity sufficient.

Questions and comments to the defense

- Why did you select NuSMV as the model checking tool? I would expect a more thorough analysis of available tools.
- In connection to the previous question: how large models are expected in practice? There is a danger of exponential run-time blow-up. Can this be a problem?
- The whole work is rather abstract. All the examples are artificially crafted. It would be nice to apply the principles to some practical (real) design. Have you tried to? If not, what were the main obstacles? Unavailability of such designs?

Final assessment

Judging from the above, it can be concluded that the applicant is highly scientifically qualified. He has proven the ability to conduct his own research and publish the results. Therefore,

I do recommend

the submitted thesis for the presentation and defense with the aim of receiving the Ph.D. degree.

In Prague, 22. 6. 2021

doc. Ing. Petr Fišer, Ph.D.
Czech Technical University in Prague
Faculty of Information Technology

Opponent's opinion on the dissertation entitled "Model-driven Security Engineering for FPGAs"
Ing. Michael Vetter

a) Evaluation of the significance of the dissertation for the field:

Intellectual property protection is one of the key knowledge for today's cyber world, not only protection against theft, but also protection against attack and degradation. In cyberspace today, it is possible to cause not only great economic damage, but loss of life.

This work includes the analysis and adaptation of appropriate security methods, originating from the software domain to the world of FPGA. The method of formalization of the FPGA security challenge (presented by the author's language FPGASECML) is described.

The work defines 5 structures (Point-to-point connection between FPGAModules, Pipelining, Bus-based Designs, Network on a chip, Gateways) of possible interconnection of modules in FPGA, their graphical expression together with the evaluation of the difficulty of breaking them. Partial runtime reconfigurations are also discussed.

Access authorization modeling in Chapter 5 is crucial for creating a control matrix of accesses to individual parts of the FPGA, rule-based access, role-based access, and access strategies.

Chapter 6 deals with the formalization of the approach to the FPGA security model.

Chapter 7 introduces a text-specific domain modeling language (DSL) that simplifies model formulation. DSL called FPGASECML, its various components and its applications, which are explained in this chapter. A simple hypothetical example with sensor, FPGA chip, configuration memory and Ethernet connection is given.

The following chapter validates the design. The first part contains scenarios for different rules. The second part discusses manual validation and the third part is a proposal for automated validation. The conversion of FPGASECML to NuSMV model containing finite state machines, rules, roles and strategies for individual parts of the system is used. Then, iteratively allows Nusmv to exclude sequences using linear time logic (LTL) that do not meet the set criteria.

Finally, Chapter 9 describes validation by converting FPGASECML to Burlap model and finding successful sequences to attack FPGA integrity using Q-learning algorithms, one of which is the Markov chain.

The working part then deals in detail with the example given in Chapter 7.

Most designers writing in HDL languages are not concerned with securing the design of the FPGA structure, which is why I consider Ing Vetter's work for the field to be very important.

b) Comments on the problem-solving procedure, the methods used and the fulfillment of the specified goal:

The doctoral student proceeds logically in steps from simpler to more complex. Defines individual threat levels (chip, printed circuit board, subsystem, system). It then elaborates the individual levels in more detail. It then performs a summary and evaluation for each level.

c) Opinion on the results of the dissertation and on the original concrete contribution of the dissertation submitter:

The contribution of the work is a thorough analysis and the resulting methodology for the design of secure systems with FPGA, but not only FPGA chips, but also for qualitatively new results covering the entire system. Although the whole process of security analysis at the theoretical level is performed in the working part, I miss at least one design of a specific real secure system with a specific FPGA chip and a test of its resistance to attack as a verification of theoretical analyzes.

d) Comments on the systematics, clarity, formal arrangement and language level of the dissertation:

The work has a clear and logical structure. It consists of two parts, overview and working, which are separated as the text of the dissertation and appendices A to H, in which the objectives and methodology are developed. In the overview part, the doctoral student started from the general basics, which he gradually develops into a more detailed form, so that he can propose their solution in the working part. The working part, as already mentioned, consists of appendices in which the doctoral student proposes scenarios for protection against hypothetical attacks. The first part of the work is summarized in Chapter 10. The working part is then in Annex H2.5. It helps clarity that the work is divided in this way, otherwise the reader would get lost in the flood of individual information. The work is written in English with a minimum of errors. In the appendix, I have noticed some nonimportant typos. Some parts deserves a more detailed explanation for the ignorant reader.

e) Comments on the student's publications:

The list of publications at the end of the thesis contains 3 items related to the results of the dissertation published in journals and books. In addition, another 7 publications at conferences. According to WOS, Michael Vetter has so far published 48 publications between 1982 and 2019. I consider this list to be sufficient.

f) Unambiguous statement of the opponent whether or not he recommends the dissertation for defense:

I recommend the thesis for defense, for which I have three supplementary questions below.

Pilsen, 23.9. Vjaceslav Georgiev

Questions for the defense:

1. Do you plan to complete your example with MDP?

2. Unstructured design methods are more demanding than structured ones. What do you propose as a methodology for finding a budgetary balance between restructuring and the risk of a system hacking?

3. FPGASECML - FPGA SECurity Model Language is your key contribution to FPGA security. Why didn't you clearly indicate that in your doctoral thesis?