ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta informačních technologií, Katedra číslicového návrhu
Thákurova 9, 16000 Praha 6

Review of a Doctoral Thesis:

Hardware Side-Channel Attacks in Safety Critical Devices

Hardwarové útoky postranním kanálem v bezpečnostně kritických zařízeních

MEng. Enrico Pozzobon

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

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

I. Thesis

Appropriateness and relevance (evaluation of the importance of the dissertation for the field)

The area of research presented in this thesis is suitable and relevant for current research challenges, especially with today's increasingly massive use of embedded systems with high demands on both security and safety. This work can help in this area and could lead to their more practical use even in safety-critical applications.

Statement on the procedure for solving the problem, the methods used and the fulfillment of the specified goals.

The main goals specified in the thesis in the pages 3 and 4 are the following:

- to classify the sources of side-channel information leakage on cryptographic algorithms running on embedded microcontroller,
- to develop a methodology to efficiently remove first-order side-channel leakages from a cryptographic algorithm on real hardware,
- to analyze the vulnerability of safety critical microcontrollers to fault injection attacks,
- to develop a system for automatically finding vulnerabilities in the code to fault injection attacks on multiple architectures.

These goals were current and ambitious. The presented goals were solved using original methods based mostly on published theoretical methods and tools, that must combine two wide not very closed areas: security and safety. Several new approaches and methods were presented and the achievements were properly verify.

But the key steps to achieve them should be more detailed and precisely described especially in the context of current trends because the contributions must be evaluated against new and very fast advancement in the presented area. The used methods (the part "state-of-the-art") would deserve a more precise description and probably also the organization of the text so that it is clearer what is the basis taken from the literature and how the own original result follows on from it.

A summary of the contributions of the thesis (opinion on the results of the dissertation and on the original concrete contribution of the submitter of the dissertation,)

The main contributions, that are presented in this thesis are:

- a discussion of different automated methodologies for automated side channel leakage removal from symmetric cryptography primitives,
- an investigation of further sources of leakages of commonly used microcontroller architectures,
- a novel search algorithm for fault-injection parameters to allow rapid evaluation of hardware for safe and secure applications.

My selection of specific results and contributions:

- The application of fault injection attacks to obtain code execution through program counter manipulation and a new algorithm for fault parameter search (makes this kind of fault injection attack feasible on black-box targets)
- The construction of an optimized 2-shares Boolean masked full adder using 12 instructions only.
- Precise experimental evaluations of proposed methods.
- The declaration of the open issues and actual and interesting future work specification focused on hardware attacks against safety critical microcontrollers used by the Automotive Industry.

Evaluation of the formal aspects of the thesis, statement on the systematicity, clarity, formal arrangement and language level of the dissertation.

The structure and organization of this thesis is logically divided into three basic parts: I. Introduction and Background, which serves as the basic introduction to the area of goals (basic principles of Side Channel Analysis and Fault Injection Attacks).

II. Side-Channel Leakage Countermeasures, where in three subchapters contributions of the thesis and research results are described: Evaluation of MCU Leakages, Boolean Masking of a Modular Adder, and their experimental evaluations.

III. Fault Injection on a MPC57xx Microcontroller, with a subchapter Evolutionary Fault Injection Algorithm, which is based on Safe and Secure Microcontrollers

The text is written in plain English. The text and descriptions are easy to read and understand. There are only several non-standard things, e.g. not fully clear and emphasizing goals and their corresponding contributions next (maybe they could have been more specific not so general). The sources are mixed with the authors original research results. It would be much better to focus and specify one or two areas of security rather than address multiple directions. In particular, I lack a clear specification of how the proposed goals were met. The "state-of-the-art" part should be much systematically described with more actual bases (not the newest and not very actual source references).

I appreciate the detailed description of the experiments verifying the described methods

II. Student's overall achievements

Quality of publications.

The research results have been published at an appropriate but not very prestigious level, as concern both the quantity and quality. But not all contributions described in the thesis were published - the work has greater publication potential.

Overall R&D activities evaluation:

I can state that Enrico Pozzbon thesis, the results included into it, his publications, and other scientific results indicate that he is a person with scientific erudition and creative abilities.

Assessment of other characteristics, reservations, comments, and questions:

- Are your fault injection methods extensible for any processors or is there any limitations?
- The list of literature and sources is neither very comprehensive nor very up-to-date (38 titles), can you comment it?
- Indicate in which of your publications your described contributions have been (specifically) published.
- See my remarks in "Quality of publications" and explain them, e.g. do you plan to prepare a new article and where do you plan to present it?
- Do you plan to widespread your results to industry?

III. Conclusion

Finally, despite of some remarks (and after their satisfactory explanations) I have to declare that PhD theses **Hardware Side-Channel Attacks in Safety Critical Devices** by MEng. Enrico Pozzbon created new methods and carefully described their evaluations. They are original ones and provide new insight on the recent digital design methods in the proposed area.

Therefore I can declare that the thesis and **MEng. Enrico Pozzbon** 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). I agree for his graduation by the title PhD.

Praha, 7. 2. 2024

Prof. Ing. Hana Kubátová, CSc.

Fakulta informačních technologií
České vysoké učení technické v Praze

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

29.01.2024

Assessment of the Ph.D. Thesis of Enrico Pozzobon, M.Sc. “Hardware Side-Channel Attacks in Safety Critical Devices “, Assessor: Prof. Dr.-Ing. Martin Hobelsberger

Mr. Pozzobon focuses in his thesis on the examination of hardware attacks on safety-critical microcontrollers and the detection as well as mitigation of those. He explores attack scenarios such as side channel attacks, proposes methodologies for detection and suppression of side channel leakages, develops techniques for automated search of fault injection vulnerabilities and provides methodologies for mitigating side channel leakages and the detection of fault injection vulnerabilities.

The thesis is very well and logically structured into parts (three) and chapters (eight chapters of text and three appendices, bibliography, and list of publications). Motivation of his work, the goals, and an outline of the thesis (chapter one) are formulated to the point. These goals are connected to the research questions formulated in the thesis exposé and fully support the approach of solving the defined research problem. All stated research questions have been answered.

The presented topic is of utmost actuality and value for the research community and application domain. With the rise and roll-out of autonomous vehicles the work, presented by Mr. Pozzobon, gains even more significance and is central to the mass roll-out of those. Throughout his thesis Mr. Pozzobon 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 the chapters two and three. Here, the author introduces side channel analysis and the most common fault injection attacks. Additional information on electromagnetic fault injection is given in chapter seven. This is all well written, logically structured and provides the technical setup for the contributions of the author in chapters four to seven.

In chapter four the focus lies on the measurement of side channel leakages. Here, different sources of information leakage present on embedded hardware are presented in detail. With use of Welch´s T-Test a technique for the detection of leakage was presented. While this is only one of a few possible leakage detection techniques and not infallible, the list of leakage sources is comprehensive and covers hardware-specific sources which are often ignored by other works in the literature. The Process of masking individual cryptographic primitives is detailed in chapter five. Here, Mr. Pozzobon presents a primitive which is more complex than the ones previously masked in the literature and therefore cannot be easily found using exhaustive search. An algorithm based on neuroevolution is used to automatically find a Boolean masking of a full-adder that is then used to construct a bitsliced modular adder, and the obtained results are used to create another informed search algorithm that finds an optimized version of the full-adder. This adder is only resistant against first-order attacks but presents a novel method and thus adds a value contribution to the research community. Further more, the considered cryptographic primitive has a larger search space than the primitives that were already shown by previous researchers, making it impossible to solve through simple exhaustive search. Chapter six compares the optimized masked gadget obtained in chapter five with the best known masked modular adder from previous works, showing a significant (26%) improvement in the encryption/decryption while also demonstrating both on simulations and on real hardware that the constructed cipher does not exhibit first-order side-channel leakages. The benchmarking of the masked cipher and its comparison with the state-of-the-art are exhaustive and show a considerable improvement to previous works in the field and the use of full ARX ciphers provide a real world utility of the presented work. Chapter seven details the development of an algorithm for automating the estimation of fault parameters in an electromagnetic fault injection attack, which is useful for deciding on the resilience of a particular piece of hardware against this type of attacks. The algorithm is shown to produce unsigned code execution on different real-world automotive ECUs targets, demonstrating a vulnerability in the ISO 14229-1:2020 standardized software update process. With the information gathering step Mr. Pozzobon shows a novel way to leak information through error stack traces. The attack shows that, counter to previous research, the "Wild Jungle Jump" attack is a viable way to attack real world devices and not just laboratory examples. To highlight this insights, the success of the attacks on real world targets demonstrates the usefulness of the work. The most important results from each chapter of the thesis are summarized and presented in chapter eight. It highlights some of the open issues left by the work and concludes with the main contributions of the work which are:

- A discussion of different methodologies for automated side channel leakage removal from symmetric cryptography primitives
- The investigation and documentation of sources of leakages of commonly used microcontroller architectures
- A novel search algorithm for fault-injection parameters

The doctoral thesis written by Mr. Pozzobon 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 six international conference papers between 2017 and 2021. Mr. Pozzobon is the leading author of two of them. All are published with co-authors. The thesis and the publication list show that Mr. Pozzobon can perform research independently. Significant parts of the work of Mr. Pozzobon´s 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/process to stay ahead of malicious parties while providing security research and methodologies open and accessible?
- How will the use of new technologies such as LLMs impact the research and real-world applications in the security field and would you approach your design of the algorithm different today (given what LLMs are now widely used and available)?

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 to real world applications and already have a meaningful impact in the industrial applications. 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