Research Affairs and Ph.D. study
Faculty of Information Technology
Brno University of Technology
Bozetechova 2
61266 Brno
Czech Republic

Forschungsgruppe
Security and Privacy

Univ.-Prof. Dipl.-Ing. Mag. Dr. techn.
Edgar Weippl
Währinger Straße 29
A-1090 Vienna

T +43-1-4277-79710
F +43-1-4277-879710
edgar.weippl@univie.ac.at
https://sec.cs.univie.ac.at/

Re 60/1493/2020 June 29, 2020
Evaluation of Dominik Malcik's Ph.D. Thesis

„Analysis of Attacks on (Micro)Chips and Development of Enhancement of their Robustness / Security“

Microchips are embedded in almost all products today, ranging from home appliance, embedded and mobile systems to distributed data centers and high-performance computing. Today, it is more economical to embed general-purpose chips into machines that perform specific tasks such as washing laundry than to design custom hardware. The particular limitations are then embedded in the firmware or the software to limit the machine's capabilities. However, many recent attacks, built on the fact that these limitations can be overcome, and functions are then executed in a way that should not be possible according to the systems' designers' plans.

In the recent past, we have seen that hardware-related attacks gain more importance, and thus, hardware-based improvements are an essential field of research. A lot of progress and research has been achieved in side-channel analysis, but much fewer results have been published on ways to manipulate the hardware protection mechanisms of chips. A possible reason is that attacks require knowledge from computer science, electrical engineering, and manufacturing. The contribution of the thesis is well summarized on page 5 and is a detailed description of how to access and understand the interior structure of a chip.

The thesis provides many details so that future researchers will be able to build on the results, which is particularly important in a topic where a lot of proprietary information is common, and access to this information for researchers is hard.
Since this line of research is not yet the main-stream in the leading security conferences, it is harder to have papers accepted at premier security conferences, and a general problem of cross-domain and interdisciplinary research is finding the best venues to publish the results and make them accessible to a diverse range of readers.
For the evaluation of the thesis, I was asked to provide answers to specific questions:

“Is the topic appropriate to the particular area of dissertation and is it up to date from the viewpoint of the present level of knowledge?”

Yes, the dissertation builds on and combines knowledge from several disciplines, such as computer science, electrical engineering, and microchip manufacturing. The bibliography is extensive, up-to-date, and contains valuable and relevant research literature.

As previously mentioned, the topic is an excellent choice and will become even more critical.

“Is the work original and does it mean a contribution to the area? – specify where the original contribution lies.”

The author published original work in several articles. The contribution is clear both from the publications and also in the thesis as described in the introduction, and there is even a subsection "1.2 Thesis Contribution" (pp4-5).

“Has the core of the doctoral thesis been published at an appropriate level?”

Yes, several papers have been published (Appendix D, p148). The fact that the papers are not published at A* security conferences such as ACM CCS, NDSS, Usenix Security, or IEEE S&P, can also be explained by the cross-domain nature of the research and that it has not yet become a main-stream topic in security research. This makes it even harder to publish in the top 4 security conferences; besides, the interdisciplinary research also should be published in multiple scientific communities, making it even harder as different research writing styles have to be taken into account.

“Does the list of the candidate’s publications imply that he is a person with an outstanding research erudition?”

Yes, the publication track record and the thesis show that Dominik Malcik is an excellent researcher in his domain and understands the academic literature and research methods in his field.

I thus strongly recommend accepting the Ph.D. thesis, and in my opinion, the candidate meets the requirements for a Ph.D. title conferment.

Univ.-Prof. Dr. Edgar Weippl

SIGNATURINFORMATIONEN		
	Unterzeichner	Edgar Weippl
	Datum/Zeit-UTC	2020-06-29T22:20:07+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument ist gemäß EU Verordnung Nr. 910/2014 (eIDAS) einem handschriftlich unterzeichneten Dokument grundsätzlich rechtlich gleichgestellt.	