
# Can I trust my machine? Modern and future challenges in the Trusting Computing domain

Submitted by

Flavio TOFFALINI

Thesis Advisor

Prof. Zhou JIANYING

ISTD

A thesis submitted to the Singapore University of Technology and Design in fulfillment of the requirement for the degree of Doctor of Philosophy

2021

# PhD Thesis Examination Committee

| | |
|---|---|
| TEC Chair: | Prof. Lu Wei |
| Main Advisor: | Prof. Zhou Jianying |
| Co-advisor(s): | Prof. Mauro Conti (University of Padua) |
| Co-advisor(s): | Prof. Lorenzo Cavallaro (King's College London) |
| Internal TEC member 1: | Prof. Sudipta Chattopadhyay |
| Internal TEC member 2: | Prof. Dinh Tien Tuan Anh |

# *Abstract*

ISTD

Doctor of Philosophy

**Can I trust my machine?**
**Modern and future challenges in the Trusting Computing domain**

by Flavio TOFFALINI

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

# Publications

Journal Papers, Conference Presentations, etc...

# Acknowledgements

The acknowledgments and the people to thank go here, don't forget to include your project advisor...

# Contents

# List of Figures

# List of Tables

*For/Dedicated to/To my...*

# Chapter 1

# Introduction

This is the introduction

# Chapter 2

# Trusting Computing Technologies

This is the background of Trusting Technologies, mainly SGX and TrustZone (?).

# Chapter 3

# Static Code Protection in Untrusted Environments

Here, I answer to the following question: **is a program loaded in memory as intended?** The answer to this question is addressed in two papers:

- Careful-Packing: A practical and scalable anti-tampering software protection enforced by trusted computing (CODASPY 2019).

# Chapter 4

# Advanced Threats for Trusting Computing

The solutions in 3 ensures that a piece of code is correctly loaded in memory. In this situation, **what could advanced threats be?**

The answer to this question is addressed in the paper:

- SnakeGX: a sneaky attack against SGX Enclaves (ACNS 2021).

# Chapter 5

# At the Edge of New Defenses for Trusting Computing

The attack described in 4 requires a study of new defenses and analyses. In particular, we would answer to the following question: **can we have evidence a program is running as intended?**

The answer to this question is addressed in three papers:

- ScaRR: Scalable Runtime Remote Attestation for Complex Systems (RAID 2019).
- SgxMonitor: A Novel Runtime Remote Attestation Schema for SGX Enclaves (under review).

# Chapter 6

# New Forensic Challenges in the Trusting Computing Domain

After discussing the attacks in 4, and see the defences in 5. I want to answer a last question, **what evidence can we extract from the memory and which conclusion do they lead to?**

- Following the evidence beyond the wall: memory forensics in SGX environment (under review).

# Chapter 7

# Conclusion

These are the conclusions.

# Appendix A

# Appendix Title Here

Write your Appendix content here.

# Bibliography

Arnold, A. S. et al. (Mar. 1998). "A Simple Extended-Cavity Diode Laser". In: *Review of Scientific Instruments* 69.3, pp. 1236–1239. URL: http://link.aip.org/link/?RSI/69/1236/1.

Hawthorn, C. J., K. P. Weber, and R. E. Scholten (Dec. 2001). "Littrow Configuration Tunable External Cavity Diode Laser with Fixed Direction Output Beam". In: *Review of Scientific Instruments* 72.12, pp. 4477–4479. URL: http://link.aip.org/link/?RSI/72/4477/1.

Wieman, Carl E. and Leo Hollberg (Jan. 1991). "Using Diode Lasers for Atomic Physics". In: *Review of Scientific Instruments* 62.1, pp. 1–20. URL: http://link.aip.org/link/?RSI/62/1/1.