EMULATION BASED SECURITY MEASUREMENT WITH APPLICATIONS IN AVIONICS, REDACTIONS, AND INDUSTRIAL CONTROL

BY

MAXWELL BLAND

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Computer Science
in the Graduate College of the
University of Illinois Urbana-Champaign, 2023

Urbana, Illinois

Doctoral Committee:

Professor Kirill Levchenko, Chair and Director of Research
Professor Adam Bates
Professor Aaron Schulman
Professor Gang Wang

ABSTRACT

The saftey of critical systems and data is of paramount importance to society. Attacks on these systems can have catastrophic consequences, and the security of these systems is often difficult to measure. Existing methods often involve access to ground-truth information, which is not always available. In this dissertation, we explore the use of emulation to measure the security of systems in the absence of ground-truth information.

Complex system emulations often require sophisticated approaches to digital forensics and tactics for navigating undecidability resulting from uncertainty of the system's state. To address these challenges, we present intelligent guess and check strategies for deducing hidden information in symbol-stripped binary firmware. Our core technical contributions are (1) the first abstract interpretation based firmware rehosting system, used to generate emulations of embedded systems. (2) A novel system for the analysis and recovery of glyph positioning information in PDF documents. This system was used to recover redacted text information where the characters were removed in hundreds of sensitive documents. (3) A logic-based intermediate representation and framework for the extraction of lifted function summaries from binary firmware. This framework makes existing verification and synthesis techniques applicable to real-world systems by translating implemented code to mathematical models. Where appropriate, we justify our strategies through discussions of correctness, precision, and generalizability. Our results are never theoretical: we apply them to pre-existing, empirically validatable domain rather than models: among others, we study the Communication Management Unit used in Boeing 737 Aircraft, historically important redacted documents, and a programmable logic controller operating a Tennessee Eastman chemical plant reactor pressure valve.

"For it is at the very moment when philosophy attempted for the first time to think rigorously the primacy of scientific knowledge that it decided to abjure precisely that aspect of thought which constituted the revolutionary character of scientific knowledge: its speculative import."
— Quentin Meillassoux, *After Finitude, p. 120.*

ACKNOWLEDGMENTS

I would like to thank my advisor, Kirill Levchenko, for pushing me to a standard of capability and achievement few attain and for maintaining his support during this process. Thank you to my committee members, Adam Bates, Aaron Schulman, and Gang Wang, for their support and guidance throughout the Ph.D., before, and in the completion of this disseration.

Thank you to Abraham Clements, Gabriela Ciocarlie, and Richard Kennell with CyManII for their support, advice, feedback, particularly in relation to the InteGreat system. Additionally, I thank my collaborators Anthea Chen, Anushya Iyer, Stephen Checkoway, Stefan Savage, Joshua Mason, YiFei Zhu, Evan Johnson, Mingjia Huo, Stewart Grant, Alex Snoeren, Anil Yelam, and Nishant Bhaskar for their support and efforts throughout our papers together, though the subjects are not all approached in this thesis. I also thank the University of Illinois, National Science Foundation, and CyManII for funding my research and efforts as a graduate student.

Additional thanks are in order for my labmates Tzu-Bin Yan, Margie Ruffin, Michael Chen, Megan Culler, Jonatas Marques, and many others at the Coordinated Science Laboratories who have provided support and friendship throughout my time at the University of Illinois, including Andrew Miller, Nikita Borisov, Michael Bailey, Deepak Kumar, Zane Ma, Paul Murley, Kyo Kim, and Joshua Reynolds. I would also like to thank my friends in the Urbana-Champaign community, including Kevin Langowski, Alex Rogers and the Ship of Fools, the Rose Bowl, Waluigi's Mansion, the Spice Rack, and other basements unnamed who supported my harsh noise wall and other musical experiments.

Finally, thank you to Annika Sornson, whose love made me realize not all systems need to be broken: unfortunately, it was too late for the redactions, airplanes, and others. Thank you as well to her parents for their support and friendship. Finally, thank you to my parents and step-parents for their love and sacrifices. Everyone mentioned above is impossible to emulate.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1. Targeted Firmware Rehosting for Embedded Systems

1.2. Glyph Positions Break PDF Text Redaction

1.3. Lifting Continuous Control Equations from Binary Code

1.4. Summary of Contributions

1.5. Dissertation Structure

CHAPTER 2

PRELIMINARIES

2.1. Abstract Interpretation

2.2. Firmware Rehosting

2.3. Guess and Check Algorithms

2.4. Information

2.5. Continuous Control

CHAPTER 3

EMULATION SYSTEMS

Emulation is the process of duplicating the outwardly observable behavior of an existing system. Emulation does not necessarily model the underlying state of the target. Simulation, on the other hand, involves modeling the underlying state of the target. The end result of a correct simulation is that simulation emulates the target system exactly. A representation used in simulation is traditionally referred to as a simulacrum: a representation of the system without the substance or qualities of the original, for example, a historical reenactment.

3.1. Hardware Emulators and Instruction Set Simulators

3.2. Functional and High Level Emulators

3.3. Intermediate Representations and Interpreters

CHAPTER 4

TARGETED FIRMWARE REHOSTING

4.1. Introduction

4.2. Related Work on Rehosting

4.3. Inferring Hardware Semantics

4.4. Program Analysis

4.5. Exploit Development

4.6. Avionics Case Study

4.7. Summary

CHAPTER 5

SIMULATION FOR DIGITAL FORENSICS

CHAPTER 6

INTERMEDIATE REPRESENTATIONS AND LIFTING

CHAPTER 7

CONCLUSIONS

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

APPENDIX A

MY APPENDIX

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Etiam lobortis facilisis sem. Nullam nec mi et neque pharetra sollicitudin. Praesent imperdiet mi nec ante. Donec ullamcorper, felis non sodales commodo, lectus velit ultrices augue, a dignissim nibh lectus placerat pede. Vivamus nunc nunc, molestie ut, ultricies vel, semper in, velit. Ut porttitor. Praesent in sapien. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Duis fringilla tristique neque. Sed interdum libero ut metus. Pellentesque placerat. Nam rutrum augue a leo. Morbi sed elit sit amet ante lobortis sollicitudin. Praesent blandit blandit mauris. Praesent lectus tellus, aliquet aliquam, luctus a, egestas a, turpis. Mauris lacinia lorem sit amet ipsum. Nunc quis urna dictum turpis accumsan semper.