

Optimizing Away Security in C

Project Report, Language-Based Security, Fall 2023, Aarhus University

Anders B. Clausen Johan T. Degn Jonathan Eilath

{clausen, johandegn, eilath}@post.au.dk

June, 2023

Abstract

Lorem ipsum...

Contents

1	Introduction	1
1.1	Related Work	1
1.2	Contributions	1
1.3	Overview	1
2	Preliminaries	1
2.1	C Compiler Optimizations	1
2.2	Side-Channel Attacks	1
3	OptiFuzz	1
3.1	Code Generation	1
3.2	Assembly Inspection	1
3.3	Fuzzing	1
3.4	Visualization	1
4	Experimental Results	1
5	Conclusion and Future Work	1
	Bibliography	2
	Appendix	3

1 Introduction

1.1 Related Work

[1]

1.2 Contributions

1.3 Overview

This paper is organized as follows: ...

2 Preliminaries

2.1 C Compiler Optimizations

2.2 Side-Channel Attacks

3 OptiFuzz

3.1 Code Generation

3.2 Assembly Inspection

3.3 Fuzzing

3.4 Visualization

4 Experimental Results

5 Conclusion and Future Work

Bibliography

- [1] Laurent Simon, David Chisnall, and Ross Anderson. What You Get is What You C: Controlling Side Effects in Mainstream C Compilers. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 1–15, 2018. doi: 10.1109/EuroSP.2018.00009.

Appendix