LLSOFTSECBOOK: AN OPEN SOURCE BOOK ON LOW-LEVEL SOFTWARE SECURITY FOR COMPILER DEVELOPERS

Kristof Beyls

EuroLLVM 2022

WHY?

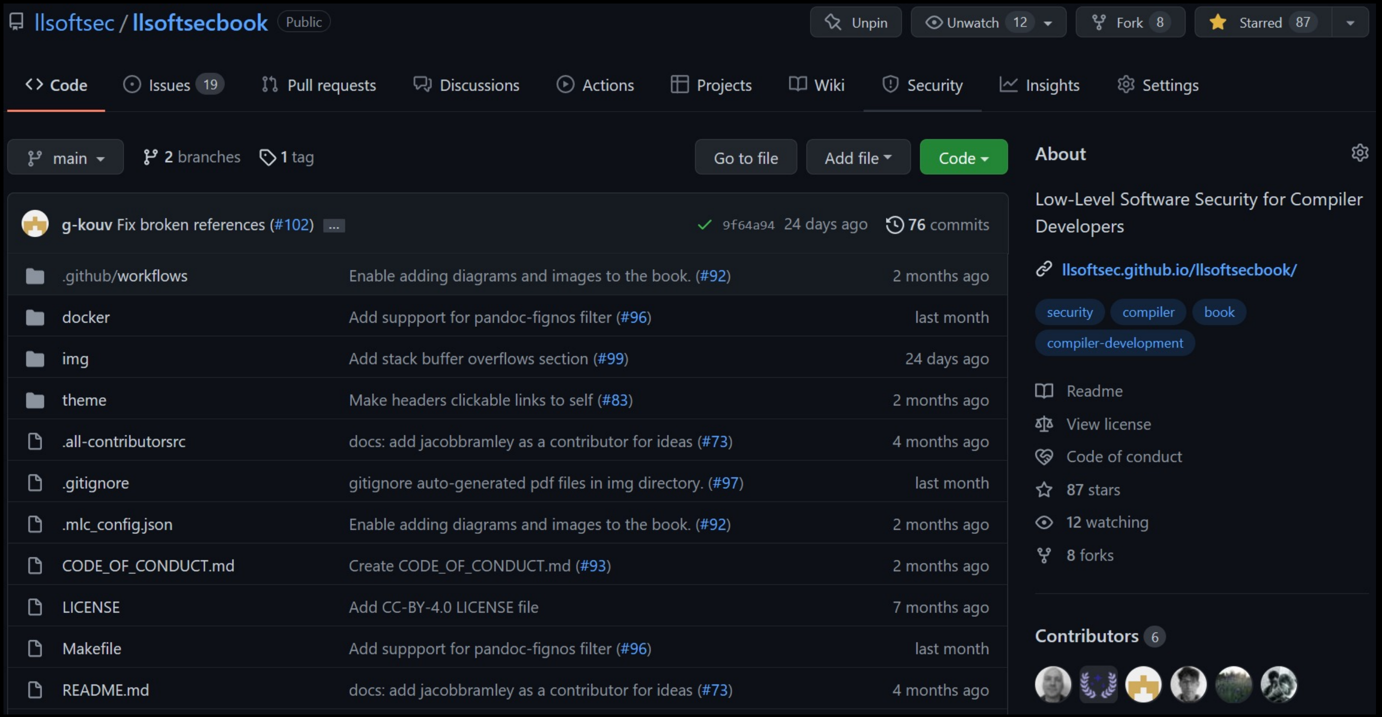
- Many compiler engineers working on security feel they lack deep enough expertise.
  - Did I really make life more difficult for attackers?
  - Could this bug be an exploitable security issue?
- We did not find good educational material
  - Lots of detailed exploits are described
  - But little material on "this is what compiler engineers should know about security"

IS IT WORTH CREATING A BOOK?

- No better way to learn about a topic then trying to describe it (Feynman technique)
- ✅ Compiler engineers are increasingly working on security features.
- ✅✅A book helps all compiler engineers, not just me.
- ✅✅✅ An open source book enables:
  - Contributions from experts where we lack expertise.
  - Might help to strengthen the network of low-level software security experts

HOW?

- Licensed under CC-BY-4.0 license
- https://github.com/llsoftsec/llsoftsecbook



llsoftsec / llsoftsecbook Public

g-kouv Fix broken references (#102) … ✓ 9f64a94 24 days ago 76 commits

.github/workflows	Enable adding diagrams and images to the book. (#92)	2 months ago
docker	Add suppport for pandoc-fignos filter (#96)	last month
img	Add stack buffer overflows section (#99)	24 days ago
theme	Make headers clickable links to self (#83)	2 months ago
.all-contributorsrc	docs: add jacobbramley as a contributor for ideas (#73)	4 months ago
.gitignore	gitignore auto-generated pdf files in img directory. (#97)	last month
.mlc_config.json	Enable adding diagrams and images to the book. (#92)	2 months ago
CODE_OF_CONDUCT.md	Create CODE_OF_CONDUCT.md (#93)	2 months ago
LICENSE	Add CC-BY-4.0 LICENSE file	7 months ago
Makefile	Add suppport for pandoc-fignos filter (#96)	last month
README.md	docs: add jacobbramley as a contributor for ideas (#73)	4 months ago

About

Low-Level Software Security for Compiler Developers

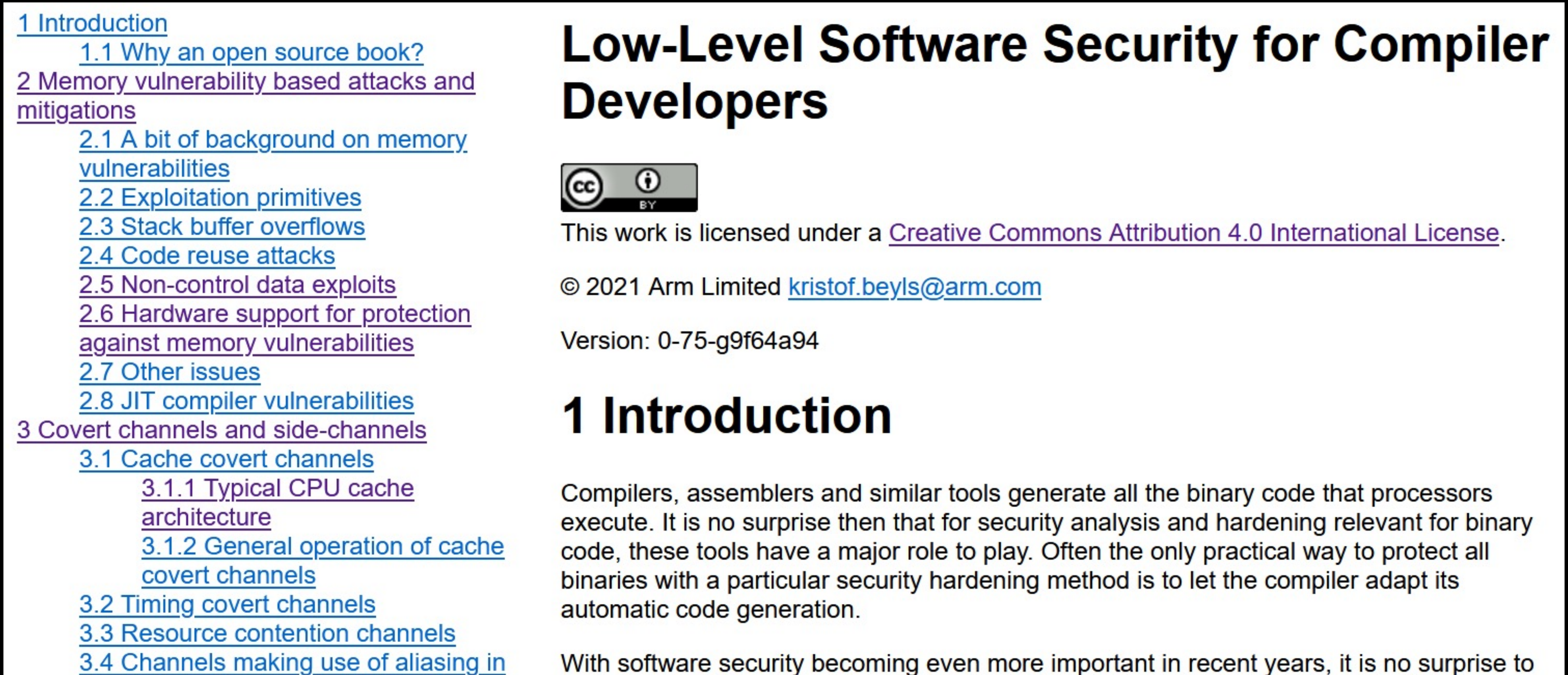
llsoftsec.github.io/llsoftsecbook/

security compiler book compiler-development

Readme
View license
Code of conduct
87 stars
12 watching
8 forks

Contributors 6

LIVE VERSION AT LLSOFTSEC.GITHUB.IO/LLSOFTSECBOOK/



Low-Level Software Security for Compiler Developers

Version: 0-75-g9f64a94

1 Introduction

Compilers, assemblers and similar tools generate all the binary code that processors execute. It is no surprise then that for security analysis and hardening relevant for binary code, these tools have a major role to play. Often the only practical way to protect all binaries with a particular security hardening method is to let the compiler adapt its automatic code generation.

With software security becoming even more important in recent years, it is no surprise to

CURRENT BOOK STRUCTURE

1. Introduction
2. Memory vulnerability based attacks and mitigations
3. Covert channels and side-channels
4. Physical access side-channel attacks
5. Remote access side-channel attacks
6. Supply chain attacks
7. Other security topics relevant for compiler developers

LOOKING FOR HELP

The project is at its start - maybe 10% of the content is present. We can use a lot of help and contributions:

- Ideas for new content.
- Any other ideas on how to improve the book.
- Review of existing content and newly written content in pull requests.
- Contributions of new sections or improvements to the text.
- Introduce your friends to this project.

How to reach out:

- Raise a github issue or start a discussion thread
- Reach out to me in any way, e.g. by email at kristof.beyls at gmail.com