Hardening Software against Physical Attacks using Static Analysis

Advisor(s): Mario Werner

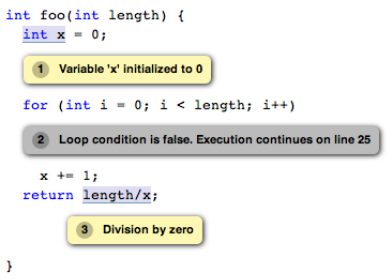
Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Austria

Motivation

Finding and fixing bugs early not only saves time but also considerably improves the quality of software. Static analysis techniques are especially useful given that they can find code smells and errors before they manifest, even in program paths which have not been exercised.
The goal of this project is to extend static analysis to the physical world. The desired static analysis tool verifies if secure coding guidelines have been followed. This enables application developers to harden their software against physical attacks without even deploying it. Source code as well as application binaries can be considered as input for the static analysis.

Goals and Tasks

- Selection of patterns which are suited for static analysis
- Selection of appropriate input format and tooling
- Implementation of the analysis
- Application of the analysis to harden a crypto library against physical attacks



Clang Static Analyzer Example

Literature

- M. Witteman
  Secure application programming in the presence of side channel attacks
  https://www.riscure.com/benzine/documents/Paper_Side_Channel_Patterns.pdf

Deliverables

- Project files (zip, cleaned)
- Documentation (pdf)
- Presentation (pdf)

Schedule

- Start Immediately
- Month 1 Reading literature
- Month 2 Implementing
- Month 3 Final deliverables

Studies

☒ INF ☒ TEL ☒ SW

Prerequisites

- C++ programming

Advisor / Contact

mario.werner@iaik.tugraz.at