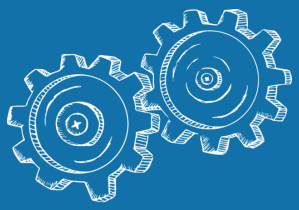


Finding Side-Channel Vulnerabilities in Crypto Libraries

Advisor: **David Schrammel, Samuel Weiser**

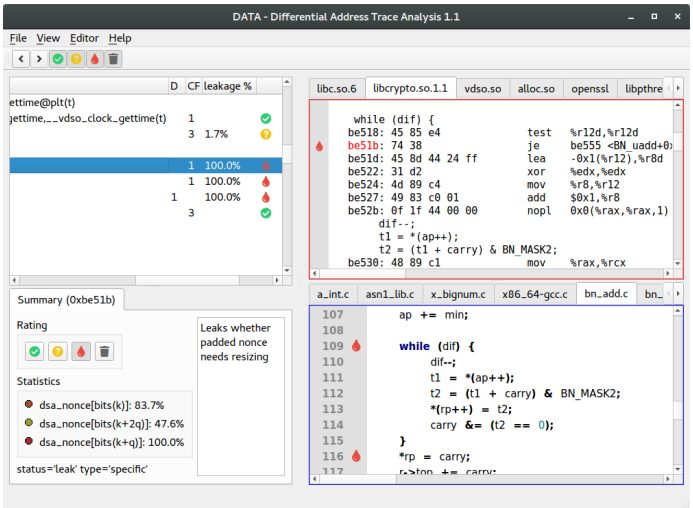
Motivation

While good cryptographic algorithms typically withstand all known real-world attacks, their implementation might be vulnerable to side-channel attacks. Several recent attacks exploit address leakage in caches, page faults or even DRAM to recover cryptographic keys, detect keyboard strokes or profile visited websites. To help mitigate these issues, we developed an analysis tool called DATA that automatically discovers such vulnerabilities [1]. We already analyzed several popular libraries like OpenSSL, LibreSSL or Google's BoringSSL and uncovered a number of vulnerabilities. Yet, there are plenty of libraries still waiting for your analysis!

In this thesis, you shall choose an open-source cryptographic library and perform side-channel analysis. This includes understanding of how DATA works, writing appropriate wrapper code and automating the process of building the respective libraries. Finally and most importantly, you shall analyze the leakage results of DATA with our GUI [2] to determine whether the discovered leakage is actually exploitable.

Goals and Tasks

- Understand software-based side-channel attacks
- Choose cryptographic library to test
- Analyze the library with DATA and the GUI



Literature

- S. Weiser et al.
  DATA - Differential Address Trace Analysis: Finding Address-based Side-Channels in Binaries
  27th USENIX Security Symposium, USENIX Security 2018, Baltimore, MD, USA, August 15-17, 2018.
- DATA-GUI
  https://github.com/IAIK/data-gui

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor Project**
Project code and documentation

☑ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- C/C++ programming
- Bash/Python/x86-assembly basics
- Interest in cryptoanalysis

Advisor / Contact

david.schrammel@iaik.tugraz.at,
samuel.weiser@iaik.tugraz.at