SIDE-CHANNEL COUNTERMEASURES FOR HOMOMORPHIC ENCRYPTION PLATFORMS

Abstract

Modern embedded devices often require access to cloud storage and computation for proper operation. Homomorphic encryption is a form of encryption that allows improved data security and privacy against untrusted cloud servers by allowing operations to be performed on encrypted data. However, embedded devices operate in a highly resource constrained environment, and typically require specialized hardware and software implementations to accelerate common operations in homomorphic encryption. These implementations are subject to various side-channel attacks, which exploit leakage of information, such as power or timing, to reveal secrets such as the encryption key. This project evaluates side-channel countermeasures, such as shuffling, in various proposed homomorphic encryption platforms. Targets are evaluated on an ARM Cortex-M4 board using side-channel power analysis on the ChipWhisperer platform. The feasibility of such countermeasures are investigated for different parameter schemes on embedded systems against know side-channel attacks.

Motivation

Homomorphic encryption is an emerging paradigm of encryption intended to increase data privacy for out-sourced storage and computation in the cloud. This is accomplished by allowing operations to be performed on the encrypted data, removing the necessity for the remote server to have access to the encryption key and subsequently the underlying data.

A major challenge in homomorphic encryption is the major performance requirements necessary to implement it. This is particularly significant in embedded environments, which have significantly fewer compute resources available. Various works have gone into optimizing the encryption operations, including FPGAs, custom SoCs, and software-based implementations such as SEAL-Embedded.

Various side-channel attacks have been performed on existing homomorphic and lattice-based encryption systems, however little work has been done investigating side-channel security in their embedded platform counterparts.

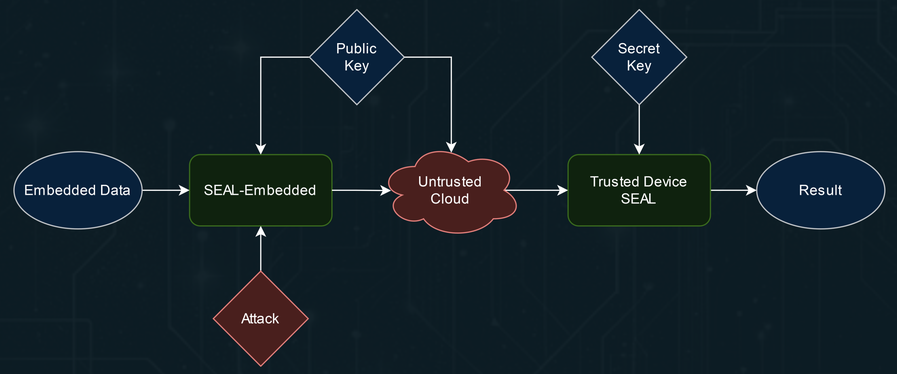
Hypothesis & Methods

This work seeks to investigate whether existing side-channel attacks can be applied to embedded homomorphic encryption platforms, as well as the feasibility of implementing corresponding countermeasures in embedded environments.

We seek to execute SEAL-Embedded, a software homomorphic encryption platform, using the ChipWhisperer side-channel hardware platform. The ChipWhisperer Lite will be used to control a STM32F3 ARM Cortex-M4 target, with power traces from the target board being captured by the CW308 UFO board.

Current Work

The hardware has been connected according to the above flowchart. The ChipWhisperer build system was modified to incorporate the SEAL-Embedded device library. Test traces have been captured to verify connectivity and functionality of the experimental setup.



Discussion

The ARM Cortex-M4 was chosen as a target due to its role as the preferred microcontroller target for post-quantum cryptography. Smaller boards may be subsequently explored to investigate highly resource-constrained environments.

Software solutions such as SEAL-Embedded may struggle to efficiently perform encryption with high-parameter schemes. Hardware SoC targets could serve more effectively in higher-security setups.

Future Work

Our immediate next steps will be establishing a simple communication interface to enable rapid iteration. We will then collect power traces to investigate possible side-channels.

Future work will explore side-channels in hardware homomorphic encryption platforms, as hardware platforms allow much higher parameter schemes, and thus improved security.

Acknowledgements

This work is funded by the DRACO Lab at the University of Central Florida.

AARON LINGERFELT
aaron.lingerfelt@ucf.edu

DRACO LAB | www.ece.ucf.edu/DRACO
Dr. Mike Borowczak, Lab Director

Dept. Of Electrical & Computer Engineering
College of Engineering and Computer Science
University of Central Florida

2023 STUDENT RESEARCH WEEK
March 27 - 31 | researchweek.ucf.edu
SHOWCASE · LEVERAGE · IMPACT · CELEBRATE

DRACO