



Collide+Power to be Continued




Advisor: **Mathias Oberhuber**

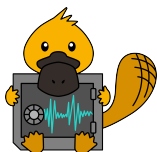
Motivation

The power consumption of a CMOS circuit depends on the processed data. Therefore, if an attacker can measure power consumption, this poses a fundamental security risk if no mitigations are in place. The Platypus attack [1] shows that unprivileged power interfaces allow an adversary to read the CPU's power consumption purely from software and enable traditional power analysis attacks on general-purpose CPUs. The resulting fixes prevent unprivileged access to this interface. However, the Hertzbleed [2] attack discovers that the CPU's execution time depends on the actual power consumption of the system and circumvents requiring access to the interface. Finally, Collide+Power [3], enhances software-based power side channels to leak arbitrary data processed by the CPU. So, where do we go from here?

We want **YOU** to extend this field! We want to explore the potential of Collide+Power even further, finding new attack targets leaking sensitive data.

Goals and Tasks

-  Read the linked literature.
-  Perform experiments on chosen CPU architecture.
-  Develop the attack to leak the data.



Literature

- > PLATYPUS: Software-based power side-channel attacks on x86
- > Hertzbleed: Turning power Side-Channel attacks into remote timing attacks on x86
- > Collide+Power: Leaking Inaccessible Data with Software-based Power Side Channels

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

- > Interest in the topic area
- > C/C++, Python, Assembly

Advisor Contact

mathias.oberhuber@iaik.tugraz.at