

# ARM TrustZone Abstraction

## Motivation

ARM TrustZone provides a secure mode on CPUs for embedded and mobile systems or smartphones. It has been used to isolate security critical code.

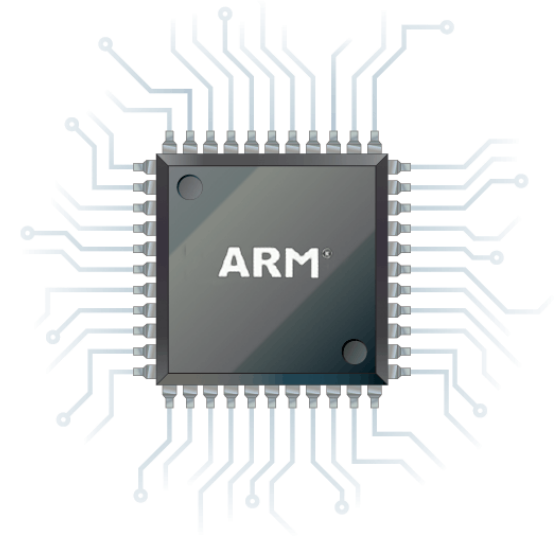
However, there is currently no technology for automatically reasoning about the security of systems built that way.

## Project description

In project you will study the CPU specifications to derive a formal model of the TrustZone mechanism.

If time permits, a formal analysis with appropriate tools against security properties will be made.

Interest in formal methods is required.



## Deliverables

- Software experiment results
- Documentation, Report
- Presentation (15-20 min)

## Scope and Credits

Studies:  INF  SEW  TEL  MATH

The scope, effort, and credits of this project are scalable.

## Advisor / contact

[ronald.toegl@iaik.tugraz.at](mailto:ronald.toegl@iaik.tugraz.at)