A journey to Soft IP Common Criteria Certification

JAIF 2020

Christophe Evrard
24/09/2020

Arm France and Arm SecurCore processor family

- Arm opened its “e-commerce design centre” in Sophia-Antipolis mid 2000 through the acquisition of EuroMIPS Systems after successful collaboration during Cascade European project.
- First homegrown project was Arm SecurCore SC100, derivative of Arm7TDMI-S processor.
- Since then, Sophia-Antipolis design centre has been home of Arm SecurCores.
- After 20 years supporting partners in their certification process, we took the opportunity of the Cortex-M35P development to consider our own IP certification.
  - Working in parallel on MSSR compliance to enable partners’ products certification.
- After 3 years from feasibility study through evaluation, both Cortex-M33 and Cortex-M35P have been certified to EAL6+ for the Common Criteria ISO 15408 standard.

Why going through evaluation of our products?

- Rise of IoT and increasing importance of security for billions of connected devices
  - See Arm's Security Manifesto
- Could we help partners' in their certification effort.
  - Specifically new entrants which are facing their first evaluation.
- Improving quality of our support
  - "Eating our own dog food".
- Unbiased, third-party security evaluation of our products
- MSSR
  - From day 1, SecurCore processors have been developed in dedicated working spaces, and dedicated IT infrastructure.
  - During Cortex-M35P requirement gathering, partners highlighted the need to comply to MSSR.

First steps

- No Soft IP have been evaluated so far.
  - Some example of evaluation of SoC subsystems, although based on Silicon.
  - Commonalities with introduction of Functional Safety in Soft IP development, leading to creation of Arm’s AE products.

- Working in partnership with certification schemes and evaluation laboratories
  - Definition of evaluation perimeter
  - Feasibility studies

- Define Security Problem Definition, Security Objectives that are relevant in the context of a Soft IP evaluation

TrustZone for Cortex-M and Cortex-M33/Cortex-M35P MPU

- ARMv8-M architecture defines Security Extensions :
  - Separation between a handler/privileged and an thread/unprivileged software execution, i.e. processor mode.
  - Partition of software and system into Secure/Trusted and Non-Secure/Untrusted worlds, i.e. processor state.
  - Rules for transitions from one state to the other, and from one mode to the other.

- In conjunction with optional MPU extension, providing memory protection based on:
  - Processor state, using two different sets of MPU region
  - Processor mode
  - Access type and address

Cortex-M35P additional security features

- In addition to ARMv8-M Security and MPU extensions, Cortex-M35P integrates specific physical security features
- Against Information leakage
  - Basic internal transfer protection
  - Subset information flow control
  - Basic internal security function protection
- Against Perturbation
  - Limited Fault tolerance
  - Failure with preservation of secure state

PP84, CC, TOE, ST, SAR, SFR, SPD, ADV, ALC, AVA, ATE… Help!

- Exposure to CC formalism, evaluation and certification process has been a definitive cultural shock for project team.

- In all fairness, Arm own formalism may have been a greater shock for evaluation lab…

- Creation of evaluation deliverables has been a long and intense process:
  - Create mutual understanding of acronyms and terms
  - Gathering of internal information in an appropriate format

- Interesting discovery of some part of own company
  - Understanding IT infrastructure and process from a user point of view.

Evaluation methods

- For claims about logical attacks against Security and MPU extensions, a model has been developed in order to prove, or give counter-example of high level assertions
  - Such as “Non-secure SW can’t read Secure Data”.

- For fault insertion attack, we faced the paradox of the “white box” approach
  - Even when mapped onto FPGA platform, access to Soft IP RTL provides _full_ controllability and observability of entire TOE.
  - On the other hand, this provide confidence that any attack can’t be performed with higher potential as perturbation can be performed on exact signal, at exact cycle.
- Vulnerabilities study led to a set of specific perturbation on a specific set of critical signals within the design.
  - HDL was subsequently modified to allow perturbation and critical asset observability.

Evaluation outcomes

- Both Cortex-M33 and Cortex-M35P have been certified EAL6+
    - First Soft IP certification standards against Common Criteria.

- Sophia-Antipolis design centre secure area has been evaluated in accordance to MSSR.

- Partners can license additional security package comprising:
    - A Security Guidance document covering TrustZone and memory protection for Cortex-M33 and Cortex-M35P, as well as an additional set of anti-tampering features for Cortex-M35P
    - A Security Target document that is developed by the product vendor (Arm) and covers the specific implementation details.
    - Verification methodology plans and summary reports
    - CC certification evaluation material for Cortex-M33 and Cortex-M35P
    - The MSSR certificate

What this certification is not!

- Since foundation of Arm SecurCore family, the only claim made about the processor family is that we are providing hooks and additional capabilities above vanilla CPUs capabilities to help partners building secure platforms.

- Current evaluations and their results can be used for composition evaluation but are in no way a guarantee of final product certification.

Q&A

- Please ask anything!