A safe & secure perspective on RISC-V and open-source hardware

Journées Nationales 2021 GDR Sécurité Informatique

Jérôme Quévremont
RISC-V and open hardware project leader
Thales Research & Technology
Thales’s Mission

Wherever safety and security are critical, Thales delivers. Together, we innovate with our customers to build smarter solutions. Everywhere.

- Sensing & data gathering
- Data transmission & storage
- Data processing & decision making
- Digital Identity and Security
- Defence and Security
- Aerospace
- Space
- Ground Transportation
Thales overview

Over 81,000 employees

68 Countries
Global presence

1 bn €
Self-funded R&D*

Sales in 2020
17 bn €

* Does not include externally financed R&D
Thales: A Research and Development Powerhouse

Albert Fert
Scientific director of the CNRS/Thales joint physics unit and winner of the 2007 Nobel prize in physics.

8 times winner

Expertise in a uniquely broad range of technical domains, from science to systems, applied across businesses.

An extensive intellectual property portfolio of 20,500 patents.
What is RISC-V?

Context

- ARM is the major player in the embedded processor market
- High licensing and royalty fees of ARM solutions + export risk

Open hardware: a credible FREE alternative

- RISC-V ISA initiative supported by 200+ members
- Credible alternative to the ARM ecosystem
- Starting point for hardware implementations
  - Open source: OpenHW Group, CHIPS Alliance...
  - Commercial: SiFive, Andes, Gaisler, Alibaba, Microchip, GreenWaves, Western Digital, Nvidia...

- Industry is moving
  - PowerPC going open source
  - MIPS adopting RISC-V ISA
  - DARPA starts to mandate RISC-V

It took 15 years to Linux for massive adoption. RISC-V has started in 2010
RISC-V ISA

- Simple & modular ISA
  - Learning from legacy (ARM, Power, x86...)
- Base: RV32I, RV64I
- Standard extensions:
  - M: multiply/divide
  - A: atomic operations
  - F, D, Q: floating-point
  - C: compressed instructions
- M/S/U privilege levels
- Virtual memory: Sv32, Sv39, Sv48
- Extensions being prepared
  - bit manip, dynamically translated languages, SIMD, vector, hypervisor, crypto...
- Room for custom/proprietary extensions
Why Thales contributes to RISC-V and open-source HW

**Software**
Large ecosystem compatible across implementations

**Security**
A fully auditable processor

**Safety**
No black-box

**No vendor-locking**
A SME business to develop custom version is being established

**Performance**
State-of-the-art processor

**SWaP & customization**
Exact fit between features and application needs

**Sovereignty**
French / European ecosystem from design to production of SoC
French members of alliances

<table>
<thead>
<tr>
<th>Companies</th>
<th>THALES</th>
<th>THALES</th>
<th>cortus</th>
<th>CHIPS ALLIANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>![Logo]</td>
<td>![Logo]</td>
<td>![Logo]</td>
<td>![Logo]</td>
</tr>
<tr>
<td></td>
<td>![Logo]</td>
<td>![Logo]</td>
<td>![Logo]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>![Logo]</td>
<td>![Logo]</td>
<td>![Logo]</td>
<td></td>
</tr>
<tr>
<td># members (worldwide)</td>
<td>42</td>
<td>100</td>
<td>19</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Research</th>
<th>CEA</th>
<th>INRIA</th>
<th>CEA</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>![Logo]</td>
<td>![Logo]</td>
<td>![Logo]</td>
</tr>
<tr>
<td></td>
<td>![Logo]</td>
<td>![Logo]</td>
<td>![Logo]</td>
</tr>
<tr>
<td># members (worldwide)</td>
<td>6</td>
<td>40</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Academy</th>
<th>ESEO</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>![Logo]</td>
<td>![Logo]</td>
</tr>
<tr>
<td></td>
<td>![Logo]</td>
<td>![Logo]</td>
</tr>
<tr>
<td># members (worldwide)</td>
<td>13</td>
<td>55</td>
</tr>
</tbody>
</table>

Engaging in alliances, a good step towards international co-operations.
1st national RISC-V student contest

Organized by

University year 2020-2021

Goal: Improve CV32A6 (32b ARIANE) FPGA performance

13 teams from 10 academies

Awards:

- 1er prix: Télécom Paris (RISCy Business team)
- Prix spécial du jury: Toulouse III (Agence Tous RISC)

Preparing 2021-2022 edition
RISC-V and open hardware @Thales

Serving global business units

OpenHW Group

- Co-Chair, Technical WG
- CVA6 (ARIANE) project leader and contributor
  - Turning ARIANE into an industrial-grade open-source IP
  - Configurable RISC-V application core: 32/64 bits, FPU or not…
  - Compatible with Linux and microkernels
  - Safe & secure orientation
  - FPGA-optimized version (softcore)

RISC-V International

- Chair, Functional Safety special interest group (SIG-Safety)
- Member of TEE, security, virtual memory committees
<table>
<thead>
<tr>
<th>Security at RISC-International</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Security committee: Identifies the needs</td>
</tr>
<tr>
<td>➢ Creates task groups: ISA extensions, crypto acceleration, trusted execution…</td>
</tr>
<tr>
<td>➢ Liaisons with: Global Platform, FIDO, Global Semiconductor Alliance, ETSI…</td>
</tr>
<tr>
<td>- E.g.: work with Global Platform to adapt TEE API for other targets, like IoT</td>
</tr>
<tr>
<td>➢ Market segment and threat model analysis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Functional Safety at RISC-International</th>
</tr>
</thead>
<tbody>
<tr>
<td>➢ Special interest group Functional Safety</td>
</tr>
<tr>
<td>➢ Identify the needs and evangelize specification TG</td>
</tr>
<tr>
<td>- Current activity: white paper drafting</td>
</tr>
</tbody>
</table>
Perfect playground

OSH and RISC-V perfect playgrounds for security research

- **Access**
  - RISC-V: Public and extendable instruction set
  - Several open-source cores (CHIPS Alliance, OpenHW Group, lowRISC...),
  - No NDA/licences needed to set up industry/academic co-operations

- **Ability to reproduce results**
- **Perfect for public scrutiny, bug hunting**

**Specific challenges:**

- **Flip side: weak solutions enable 0-day attacks**
- **Attackers could inject malware in open-source repositories**

Certification

- Easier path to safety or security certification
  - With open-source verification artefacts (test plans, test benches and sequences)

- Increasing HW vulnerabilities
  - Remember Spectre/Meltdown breakthrough
  - Need stronger security assurance and resistance against analysis
Formal methods

- **Formal verification gaining momentum in RISC-V communities**
  - Propelled by open-source research on formal models and tools
    - SRI International, U. Cambridge, Bluespec, Yosys...
  - Bring more trust: covering 100% of states/inputs/conditions

- **RISC-V Sail formal model**
  - RV32I, RV64I, common extensions (M, A...), privilege modes, virtual memory (Sv32, Sv39...), FP (partial)
  - On-going work: “implementation choices”, new extensions...

- **Examples of security applications**
  - Detect flaws: privilege escalation, gaps in data separation, exotic corner cases...
  - Trojans
  - ISA compliance

- **Links:**
  - RISC-V formal model written in Sail: https://github.com/rem-sproj/sail-riscv
  - Sail tools: https://github.com/rem-sproj/sail
  - Tutorial: https://github.com/rsnikhil/RISCV_ISA_Spec_Tour
  - Yosys tools: https://github.com/YosysHQ
Various security work (1/2)

**RISC-V crypto extensions**
- On-going at RISC-V International
- Improve performance for common algorithms (AES, SHA…)
- [https://wiki.riscv.org/display/TECH/Cryptographic+Extensions+TG](https://wiki.riscv.org/display/TECH/Cryptographic+Extensions+TG)

**Architectural protection**
- Adding countermeasures: HW, SW, compiler-assisted, enclaves…
- "**Morpheus**: A vulnerability-tolerant secure architecture based on ensembles of moving target defenses with churn"
  - Gallagher, M., Biernacki, L., Chen, S., Aweke, Z. B., Yitbarek, S. F., Aga, M.T., ... & Austin, T. (ASPLOS’19)
- "**Keystone**: An open framework for architecting trusted execution environments"
Various security work (2/2)

**seL4**
- A separating microkernel for security and safety
- Formally verified, verified on RISC-V in 2020
- Implemented on ARIANE core (CV64A6)
- Gernot Heiser, U. South Wales & seL4 Foundation, [https://sel4.systems](https://sel4.systems)
- RISC-V week 2021 keynote ([https://open-src-soc.org/2021-03/media/slides/3rd-RISC-V-Meeting-2021-03-30-09h00-Gernot-Heiser.pdf](https://open-src-soc.org/2021-03/media/slides/3rd-RISC-V-Meeting-2021-03-30-09h00-Gernot-Heiser.pdf))

**FENCE.T**
- Temporal fence to protect against SPECTRE-like attacks
- ARIANE custom extension
Food for thought

- Hypervisor (H) privilege level
  - Not yet ratified

- Full SoC perspective, beyond the core
  - Protecting memories, peripherals, interconnects
  - Enforcing separation…

- Tooling (GCC, LLVM…), IDE (Eclipse…), electronic CAD

- Permanent RAM: new programming paradigm
Questions?