SCARV: a side-channel hardened RISC-V platform

https://github.com/scarv

Daniel Page
Department of Computer Science, University of Bristol,
Merchant Venturers Building, Woodland Road,
Bristol BS8 1UB, United Kingdom.
csdsp@bristol.ac.uk

21/11/19

CERBERUS Security Laboratories

University of BRISTOL

THALES

- Recap:

$$\begin{aligned}
\text{SCARV} &\simeq \text{RISC-V} + \text{cryptography} \\
&\simeq \text{RISC-V} + \text{cryptographic engineering} \\
&\simeq \text{RISC-V} + \text{implementation} + \text{implementation attacks}
\end{aligned}$$

where

$$\begin{aligned}
\text{WP-A} &\simeq \text{a side-channel resistant RISC-V implementation} \\
\text{WP-B} &\simeq \text{RISC-V support for next-generation cryptography} \\
\text{WP-C} &\simeq \text{a democratised side-channel evaluation lab.}
\end{aligned}$$

- Summary:
  1. XCrypto: a cryptographic ISE for RISC-V.

     https://github.com/scarv/xcrypto

     - accelerate software-based cryptographic workloads vs. base ISA,
     - allow flexibility wrt. parameterisation, countermeasures, etc.
     - example: multi-precision integer arithmetic

$$\texttt{xc.mmul.3 (rd2, rd1), rs1, rs2, rs3} \;\Rightarrow\; \left\{ \begin{array}{l} t \leftarrow (\mathsf{GPR}[\texttt{rs1}] \times_u \mathsf{GPR}[\texttt{rs2}]) +_u \mathsf{GPR}[\texttt{rs3}] \\ \mathsf{GPR}[\texttt{rd1}] \leftarrow t_{\mathrm{XLEN}-1\ldots0} \\ \mathsf{GPR}[\texttt{rd2}] \leftarrow t_{2\cdot\mathrm{XLEN}\ldots\mathrm{XLEN}} \end{array} \right.$$

     - involved with RISC-V Cryptographic Extensions Task Group wrt. a standard scalar (vs. vector) ISE.

- Summary:

  2. Micro-architectural design $\Longleftrightarrow$ (analogue) information leakage.
     - micro-architectural impact on share slicing in masked implementations,
     - FENL: a fence for micro-architectural leakage.

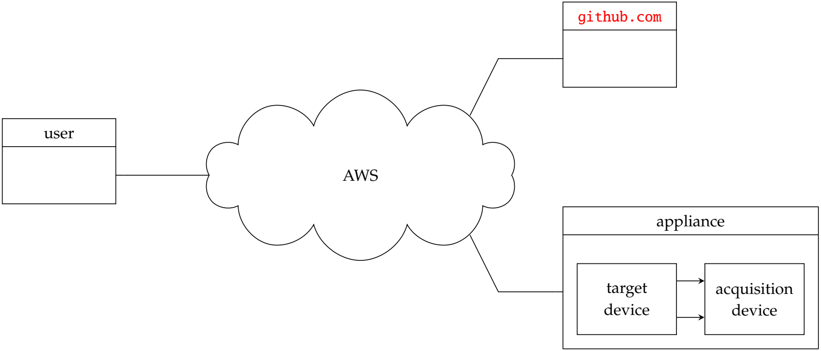
- Summary:
  3. SCARV: a side-channel hardened RISC-V micro-controller.

     https://github.com/scarv/scarv

     - RISC-V compatible, RV32IMC-based processor core plus SoC,
     - test-bed for XCrypto, FENL, etc.
     - in-progress Zephyr port ⇝ demonstrator(s).

https://www.zephyrproject.org

- Summary:
  4. SCA3S: Side-Channel Analysis as a Service.



  - Continuous Integration (CI) mode ≃ “LGTM for side-channels”[1],
  - build-it, break-it, fix-it [1] contests (e.g., CHES challenge),
  - ...

https://semmle.com/lgtm

Questions?

References

[1] A. Ruef et al. "Build It, Break It, Fix It: Contesting Secure Development". In: *Computer and Communications Security (CCS)*. 2016, pp. 690–703. URL: http://builditbreakit.org (see p. 6).