SCARV: a side-channel hardened RISC-V platform

https://github.com/scarv

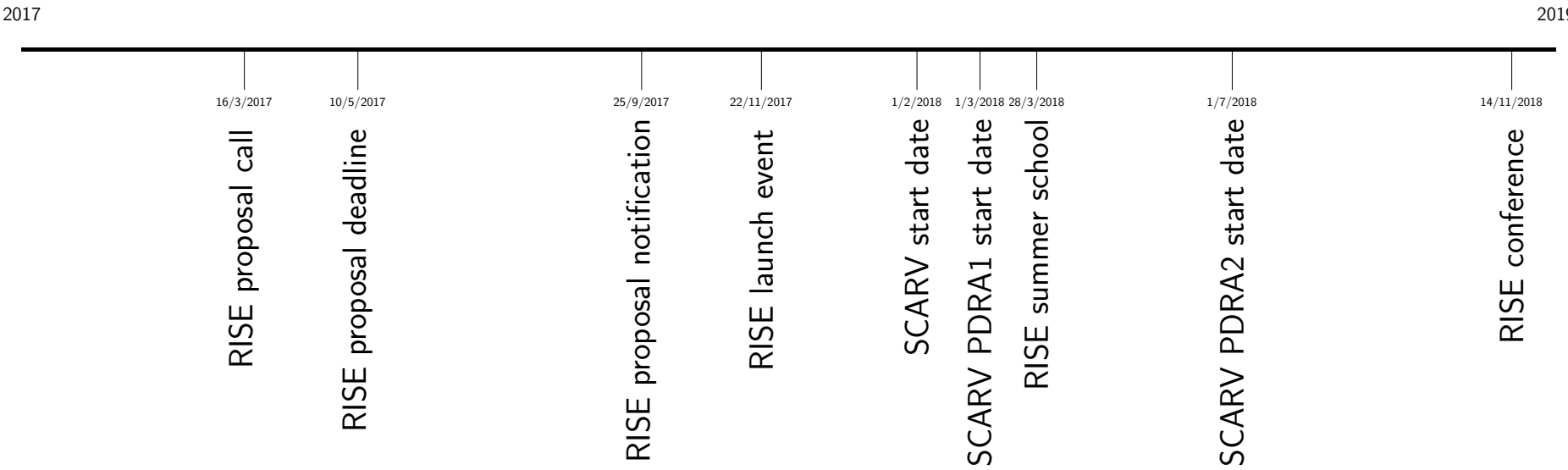
Daniel Page
Department of Computer Science, University of Bristol,
Merchant Venturers Building, Woodland Road,
Bristol BS8 1UB, United Kingdom.
csdsp@bristol.ac.uk

14/11/18

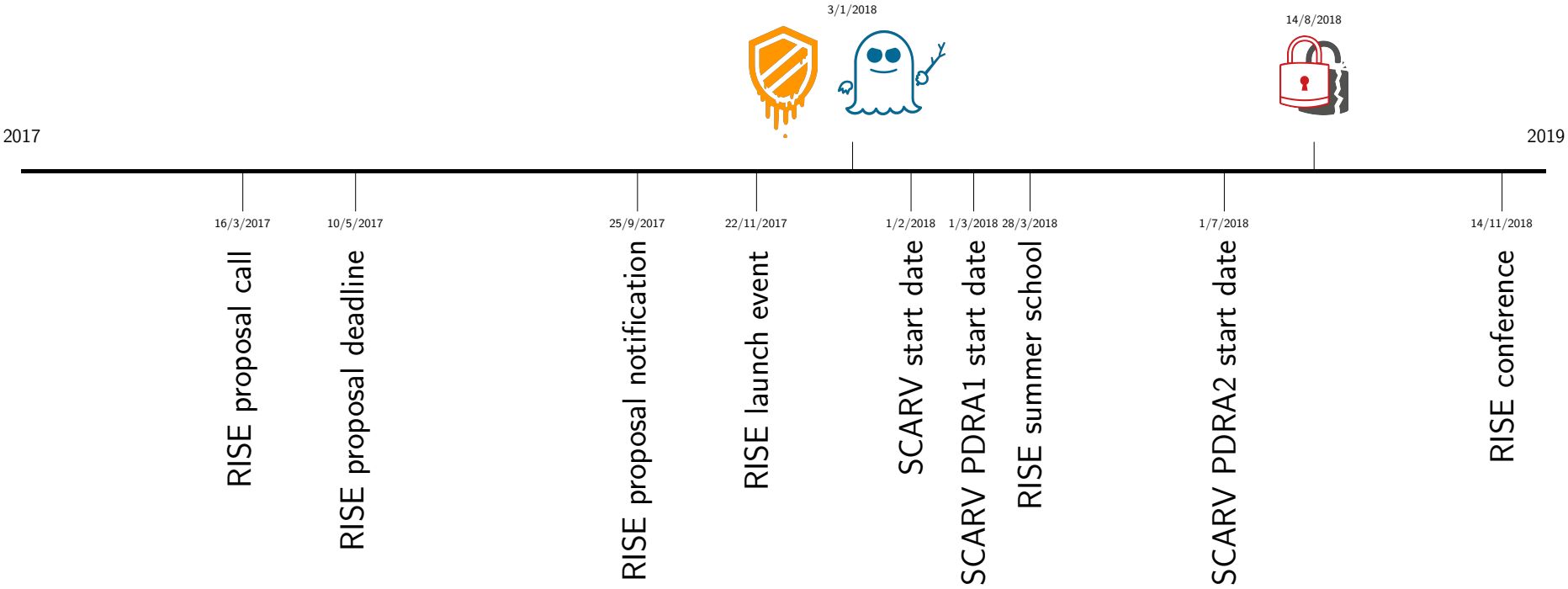
CERBERUS
Security Laboratories

University of BRISTOL

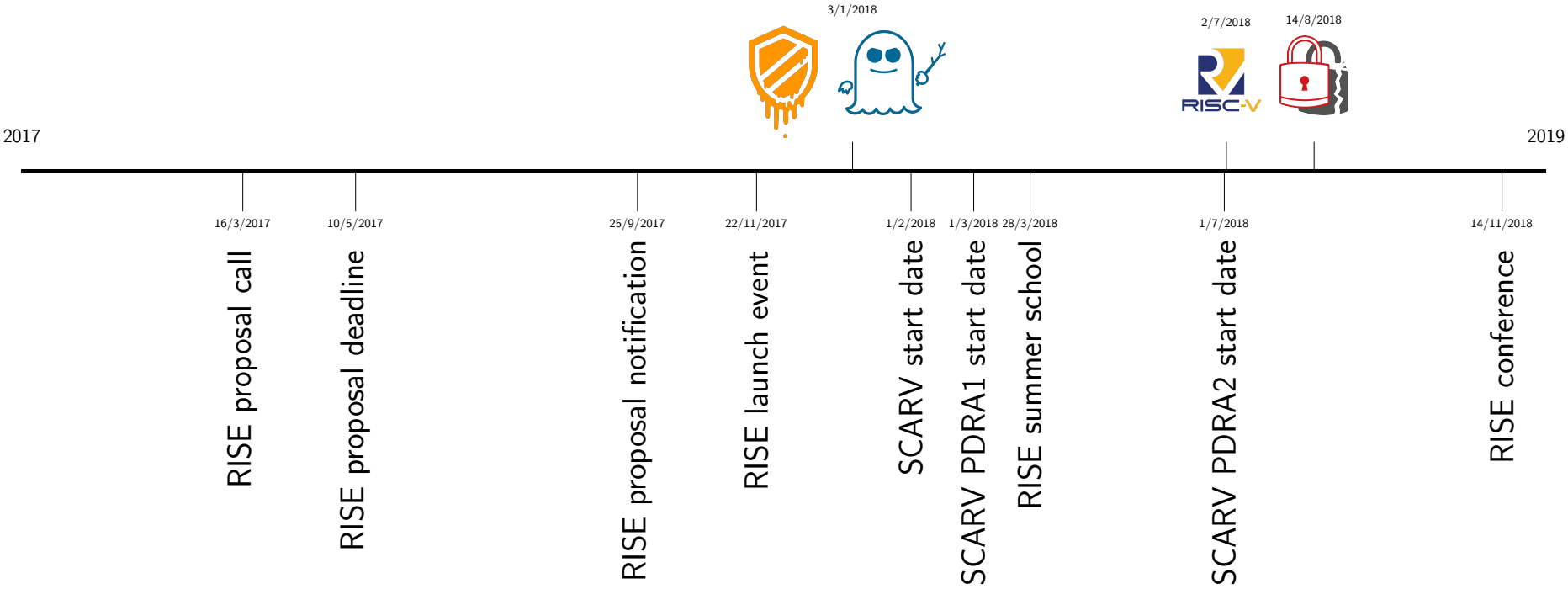
THALES



https://www.ukrise.org



https://meltdownattack.com https://spectreattack.com https://foreshadowattack.eu



https://riscv.org/2018/07/risc-v-foundation-announces-security-standing-committee-calls-industry-to-join-in-efforts

- What we *said* we'd do:

WP-A
≡
a side-channel resistant
RISC-V implementation

- side-channel hardened implementation techniques (e.g., vs. DPA),
- side-channel aware ISA design (cf. [5, 3]),
- design transparency ⇒ more accurate leakage modelling.

- What we *said* we'd do:

WP-B
≡
RISC-V support for
next-generation cryptography

- domain-specific (micro-)architectural design,
- support for implementation of light-weight and post-quantum cryptography,
- (secure) design and use of embedded FPGA fabric (e.g., EFLX, per [1], cf. [2, 4]).

- What we *said* we'd do:

WP-C
≡
a democratised
side-channel evaluation lab.

- cloud-based leakage assessment (simulated and real platform),
- "build-it, break-it, fix-it" [6] style contest.

- What we *did* do (in 2018/Q1 to 2018/Q3):
  1. started some new work, e.g.,

     WP-A: cryptographic ISE design and reference implementations

     https://github.com/scarv/xcrypto

     WP-A: BSP-like experimental infrastructure

     - cores : PicoRV32, Rocket Core, . . .
     - boards : Arty, iCEstick, SAKURA-X, Zebo, ZedBoard, . . .

     WP-A: support for hiding-based countermeasures against DPA-like attack,
     WP-C: prototype AWS-based acquisition infrastructure.

- What we *did* do (in 2018/Q1 to 2018/Q3):

2. continued some previous work, e.g.,

   https://github.com/danpage/mascab

   and

   https://github.com/danpage/scale

Questions?

References

[1] P. Clark. *SiFive signs Flex Logix for low-cost FPGA fabric*. 2017. URL: http://www.eenewseurope.com/news/sifive-signs-flex-logix-low-cost-fpga-fabric (see p. 6).

[2] M.W. Dales. "Managing a reconfigurable processor in a general purpose workstation environment". PhD thesis. 2003 (see p. 6).

[3] Q. Ge, Y. Yarom, and G. Heiser. "No security without time protection: we need a new hardware-software contract". In: *Asia-Pacific Workshop on Systems (APSys)*. 2018 (see p. 5).

[4] P. Grabher et al. "An exploration of mechanisms for dynamic cryptographic instruction set extension". In: *Cryptographic Hardware and Embedded Systems (CHES)*. LNCS 6917. Springer-Verlag, 2011, pp. 1–16 (see p. 6).

[5] G. Heiser. "For Safety's Sake: We Need a New Hardware-Software Contract!" In: *IEEE Design & Test* 35.2 (2018), pp. 27–30 (see p. 5).

[6] 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. 7).