In modern computing platforms, power monitors are employed to deliver online power estimates to support different run-time power-performance optimization methodologies. However, the possibility of setting up a successful side-channel attack (SCA) by analyzing the power estimates, imposes the use of a suitable and systematic approach in the design of such power monitors.

The presentation addresses the importance of providing accurate power monitors for cores and accelerators composing an edge platform, focusing on the benefits of implementing in hardware such components.

However, in order to prevent the possibility to exploit such information to mount a side-channel attacks, it will be presented a methodology to create side-channel resistant power monitors, automatically.

Our validation leverages both CPA and t-test analysis considering a general purpose System-on-Chip executing different cryptographic primitives and an application-specific accelerator implementing the AES-128 algorithm.

Considering several temporal resolutions, we achieved an accuracy error of the power estimates limited to less than 2.7%, as well as an average area and power overheads for the protected power monitors lower than 6% and 5%, respectively.

It is also presented a startup company, Blue Signals, commercializing tools to analyze the vulnerability to side channel attacks of hardware platforms. Beside the secure power monitor generator, an important tool, called “Inspect”, allows to identify the parts of the hardware design that are responsible of the information leakage, to implement the proper countermeasures.

Papers on the secure hardware power monitor

L.Cremona, W.Fornaciari, D.Zoni, Automatic identification and hardware implementation of a resource-constrained power model for embedded systems. Sustainable Computing: Informatics and Systems, Vol. 29, Part B, 2021, https://doi.org/10.1016/j.suscom.2020.100467.

D. Zoni, L. Cremona and W. Fornaciari, "Design of side-channel resistant power monitors," in IEEE TCAD, 2021. https://doi.org/10.1109/TCAD.2021.3088781.

More on the HEAP Lab

https://heaplab.deib.polimi.it/

More on the Startup Blue Signal and the Inspect tool

Blue Signals Srl – an innovative startup and a Politecnico di Milano spin-off – https://bluesignals.it