DVFS covert-channels in Zynq Ultrascale+ SoC-FPGAs

CARLOS ANDRES LARA-NINO,

Univ Lyon, UJM-Saint-Etienne, CNRS. Laboratoire Hubert Curien UMR 5516, F-42023, France.

The security of a System-on-a-Chip (SoC) relies on multiple isolation layers. Externally, it is necessary to prevent physical access to the device so that potential attackers cannot conduct analysis of its side channel footprints. Internally, it is common practice to implement strategies like Trusted Execution Environments (TEE) where sections of the device are excluded from interacting with the others. In the case of Xilinx' SoC-FPGAs, it is possible to create secure enclaves in the processing system (PS) using technologies like the ARM's Trusted Framework-A and the Open Portable Trusted Execution Environment (OP-TEE). The programming logic (PL) is then protected with extensions of these technologies, like TrustZone, which are meant to enforce access policies so that the interaction between untrusted/trusted applications and hardware components are limited. However, the possibility of creating covert channels within the SoC threatens these isolation paradigms. These covert channels can be exploited to transfer information between components which are not meant to be able to exchange information. Among other approaches, it has been shown that it is possible to create covert channels by exploiting the Dynamic Voltage and Frequency Scaling (DVFS) technology available in modern SoC-FPGAs. These attacks are devastating since these platforms share a Power Distribution Networks which provides the medium for the implementation of DVFS covert-channels. An attacker might be able to leverage vulnerabilities in the SoC's firmware, the operating system, or the design tools to gain access to the voltage regulators and PLLs which perform the voltage and frequency modulation. The Linux operating system is particularly vulnerable in this regard. This talk describes, for the very first time, the implementation and simulation of DVFS covert-channel attacks in Zynq Ultrascale+ SoC-FPGAs.

Author's address: Carlos Andres LARA-NINO,

Univ Lyon, UJM-Saint-Etienne, CNRS. Laboratoire Hubert Curien UMR 5516, F-42023, 18 rue Benoit Lauras 42000, 18 rue du Professeur Benoît Lauras 42000, Saint-Étienne, France., carlos.lara@univ-st-etienne.fr.