IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 November 2022, accepted 19 December 2022, date of publication 22 December 2022,
date of current version 29 December 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3231753

RESEARCH ARTICLE

DFAulted: Analyzing and Exploiting CPU Software Faults Caused by FPGA-Driven Undervolting Attacks

DINA G. MAHMOUD[1], (Member, IEEE), DAVID DERVISHI[1], SAMAH HUSSEIN[1], VINCENT LENDERS[2], (Member, IEEE), AND MIRJANA STOJILOVIĆ[1], (Senior Member, IEEE)

[1]School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne (EPFL), 1015 Lausanne, Switzerland
[2]Cyber-Defence Campus, armasuisse, 3602 Thun, Switzerland

Corresponding author: Dina G. Mahmoud (dina.mahmoud@epfl.ch)

This research is supported by armasuisse Science and Technology.

ABSTRACT Field-programmable gate arrays (FPGAs) combine hardware reconfigurability with a high degree of parallelism. Consequently, FPGAs offer performance gains and power savings for many applications. A recent trend has been to leverage the hardware versatility of FPGAs with the software programmability of central processing units (CPUs) to improve the performance of processing-intensive workloads. A variety of heterogeneous FPGA-CPU embedded systems are thus available. However, the security of FPGA-CPU systems has not yet been thoroughly evaluated. In this work, we demonstrate the first attack on FPGA-CPU platforms which leverages undervolting caused by the FPGA to inject faults and exploit them against a software encryption algorithm. The aggressor FPGA affects a CPU sharing the same system-on-chip (SoC). We show that circuits in the FPGA fabric, controlled by an attacker, can create a significant supply voltage drop which, in turn, faults the software computation performed by the CPU or even causes