Remote Dynamic Partial Reconfiguration for Emerging IoT applications: Threats and Countermeasures

Abstract

The Internet of Things (IoT) is a dynamic, ever-evolving "living" entity. Hence, modern Field Programmable Gate Array (FPGA) devices with Dynamic Partial Reconfiguration (DPR) capabilities, which allow in-field non-invasive modifications to the circuit implemented on the FPGA, are an ideal fit for emerging IoT applications. Remote Dynamic Partial Reconfiguration (RDPR) of FPGAs is a modern technique which allows "in–field", "on–the–fly" modifications to predefined partitions of the FPGA floorplan from a remote device connection. In this technique bitstreams corresponding to a new "add-on" hardware is transferred over a remote connection to the deployed FPGA. Controllers residing within the FPGA initiates Dynamic Partial Reconfiguration (DPR) in the required FPGA partition, whereby a new hardware design gets configured for use. The RDPR of FPGAs provides countless benefits as it allows mapping of additional hardware to the device as and when required, with out the need of bringing the FPGA "off–line" or without the need of storing bitstreams inside the FPGA.

In this work we propose a novel complete methodology for RDPR of FPGAs in IoT applications using open source software packages, and standard EDA/CAD software tools which do not require special paid license for establishing RDPR. This feature may be exploited by an adversary to launch attacks on the device. We further analyze the security threats on the proposed RDPR systems mainly due to malicious bitstreams corresponding to Hardware Trojan Horses (HTHs). HTHs are malicious hardware alterations in the device which would either effect the circuit functionality or leak useful information via a covert channel. In this thesis, we also provide low-overhead solutions based on Physically Unclonable Functions (PUFs) to resist these threats.

Keywords: Internet of Things (IoT), Dynamic Partial Reconfiguration (DPR), Remote Dynamic Partial Reconfiguration (RDPR), Field Programmable Gate Arrays (FPGAs), Hardware Trojan Horse (HTH), Physically Unclonable functions (PUFs).