Embedded OS for FPGA platform: a Hardware-to-Software Security Overview

Florian Devic
SAS NETHEOS &
LIRMM UMR - CNRS 5506
University of Montpellier 2
Montpellier, FRANCE
Email: f.devic@netheos.net

Lionel Torres
LIRMM UMR - CNRS 5506
University of Montpellier 2
Montpellier, FRANCE
Email: lionel.torres@lirmm.fr

Benoît Badrignans
SAS NETHEOS
Montpellier, FRANCE
Email: b.badrignans@netheos.net

Abstract

Nowadays, embedded applications require more and more advanced OSs (Operating Systems). Indeed, Linux is becoming increasingly popular in embedded world. Due to the reconfiguration feature, growing performances and low development costs, FPGAs (Field-Programmable Gate Arrays) are widely used for embedded systems. This trend is growing up.

They are used for a wide spectrum of applications. For instance, FPGAs are used in electronic consumer, automotive, space and military devices to run in diversified environments, often highly connected and exposed to several attacks. These embedded systems are attacked for intellectual property theft targeting set-top boxes, spying or taking control for automotive, space and military applications.

Embedded systems may be unpackaged, and attacked on every levels from hardware to software and on all interfaces. In general the main problem is that they communicate and require to be updated through potentially insecure channels.

That is why such devices need to be protected thanks to counter-measures providing integrity, confidentiality and authentication while ensuring system freshness and resources isolation.

This motivates a survey about the protection mechanisms existing in the state of art for FPGA devices from the bitstream configuration process to the application running on the embedded OS.

In the aim to propose an overview of actual counter-measures, this survey enumerates and explains how to protect embedded systems and more particularly FPGA-based embedded systems taking remote updates into account.