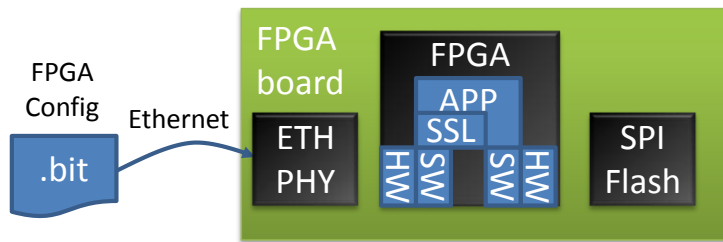


MASTER THESIS:

“Secure FPGA Update”

Motivation

FPGAs with network interfaces allow complex distributed systems. Such devices require remote update of their configuration fulfilling decent security demands.



This master thesis refines a concept for secure firmware updates and provides an implementation on Xilinx FPGAs. The project has the following requirements:

- Protocol for firmware transmission
 - Authentication and encryption (TLS?)
 - Simple IP stack (LwIP)
 - Reuse of existing Ethernet interface
- Flash programming (SPI)
 - Fallback to old version on failure
- Little footprint (minimal HW and SW resources)
 - Own FPGA setup for update

Goals and Tasks

- Check proposed concept for applicability
 - Communication layers
 - Crypto: Authentication and encryption
 - Xilinx FPGAs and SPI flash
- Pure software demonstrator (C/C++)
 - Interfacing of LwIP and TLS
- Mapping to target platform
 - Xilinx FPGA board (Spartan6 or Virtex6)
 - Microblaze CPU
- Optimization goals
 - Reuse of Xilinx resources (MultiBoot)
 - Reuse of SW stack (LwIP)
 - Reuse of crypto SW (TLS)
 - Low resource usage (LUTs, BRAM)

Payment

Single payment of € 2750,- (Werkvertrag) in case of success. Eventual bonus of 500,-.

Literature

- [1] Wikipedia, [Comparison of TLS implementations](#), 2011.
- [2] Xilinx Inc., [LightWeight IP \(LwIP\) Application Examples](#), XAPP1026, <http://www.xilinx.com/>, 2011.
- [3] Xilinx Inc., [Spartan-6 FPGA Configuration](#), User Guide UG380, <http://www.xilinx.com/>, 2011.
- [4] Xilinx Inc., [SP605 MultiBoot Design](#), Reference Design RDF0028, <http://www.xilinx.com/>, 2011.

Deliverables

- Project files (.zip, cleaned)
 - HW: Verilog sources
 - SW: ANSI C sources
- Documentation (inline)
- Tutorial (getting started)
- Presentation (.ppt 20 min)
- Written thesis (60+ pages)

Project Schedule

- Start: Now
- Month 1: Read literature, project plan
- Month 2: Adapt concept
- Month 3-5: Implement concept
- Month 6: Write thesis

Studies

- Telematik

Prerequisites

- LV System-on-Chip Architectures
- LV VLSI Design

Advisor / Contact

xFace Dr. Johannes Wolkerstorfer (project advisor)
Johannes.Wolkerstorfer@xface.at

IAIK Dr. Michael Hutter (thesis advisor)
Michael.Hutter@iaik.tugraz.at