FPGA-Rootkits

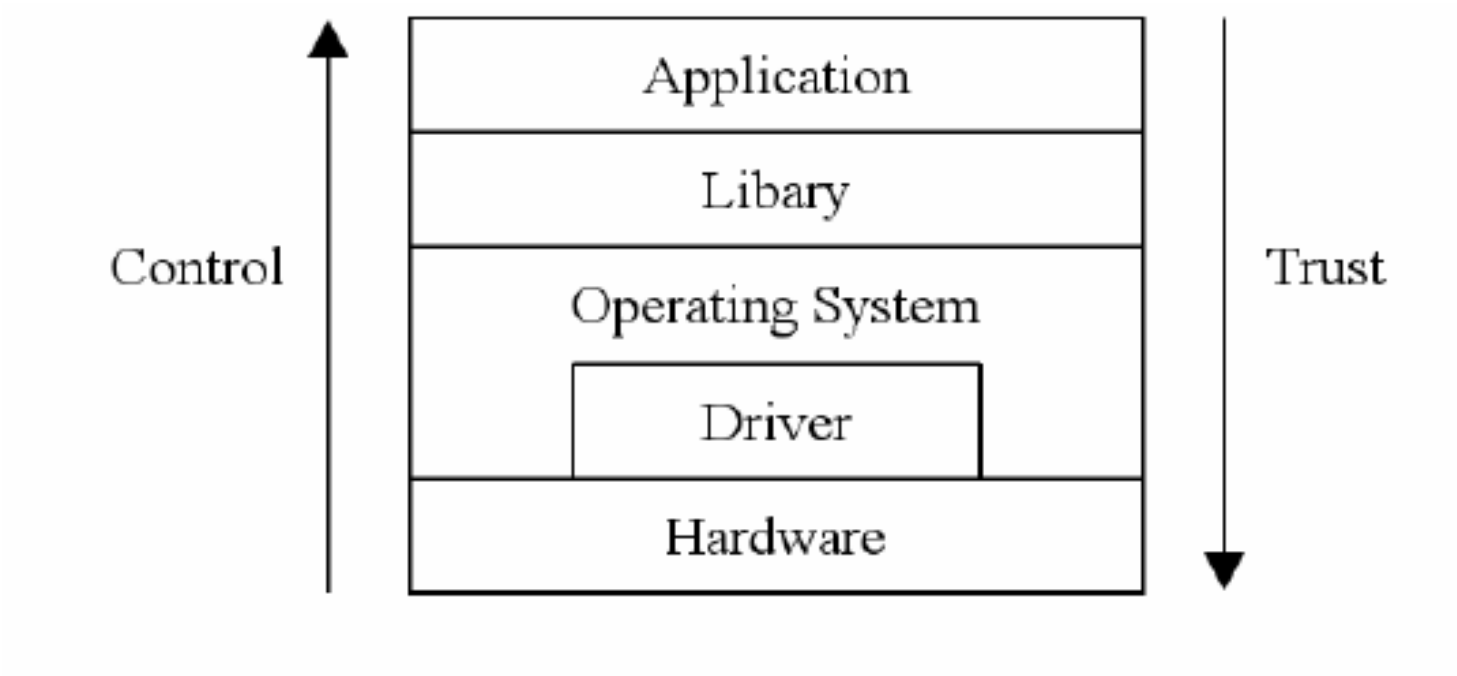
Markus Kucera

Michael Vetter

Agenda

- Introduction to Rootkits
- Security Measures in FPGAs
- Rootkits in FPGAs

Rootkits
Trusted Computing Base



Rootkits
Trends

- As old as the first Unix-Hacks
- Growing Threat in the PC-World
- New development: Hardware based Rootkits
  - ACPI-Rootkit
  - PCI-Rootkit

Rootkits
Example for Embedded System

- FPGA used for cryptographic operations in HDTV
- Hacker injects own code to circumvent encryption
- HD-Stream open for everyone

Security Measures in FPGAs I

- Encryption of the Datastream
- Authentication of the Datastream
- Authentication of the FPGA config. Itself

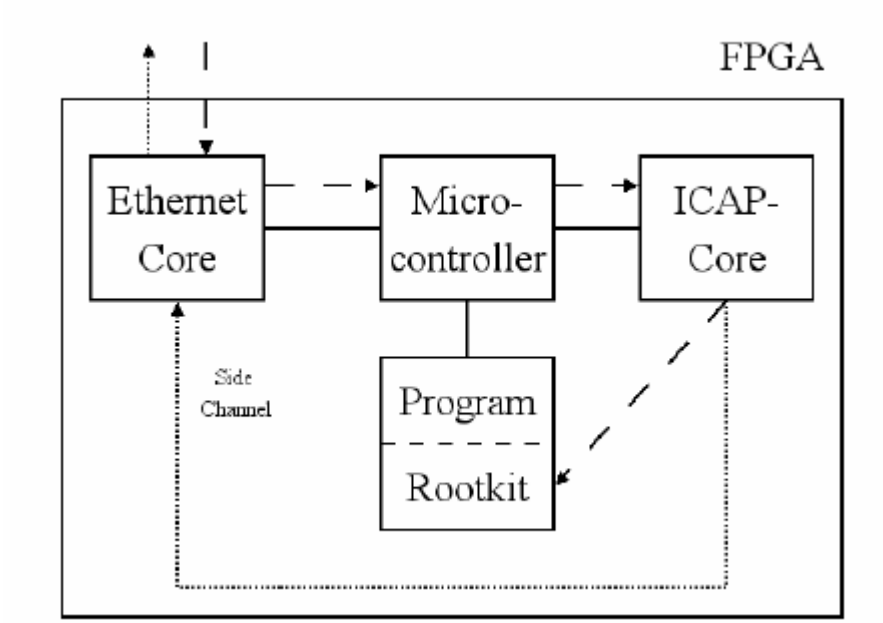
Security Measures in FPGAs II

- Authorization of the Programming Device
- Access Control

Security Threats

- Man-in-the-middle-Attack
  - Eavesdropping of Messages
  - Changing of Messages
- Replacement/Bypassing of existing Code

Deployment of Rootkits - Example



Resume

- Security Measures for FPGAs are unsufficent
- Comprehensive security Architecture necessary
- Ongoing work:
  - Evaluation of different Security Scenarios
  - Development of appropriate countermeasures