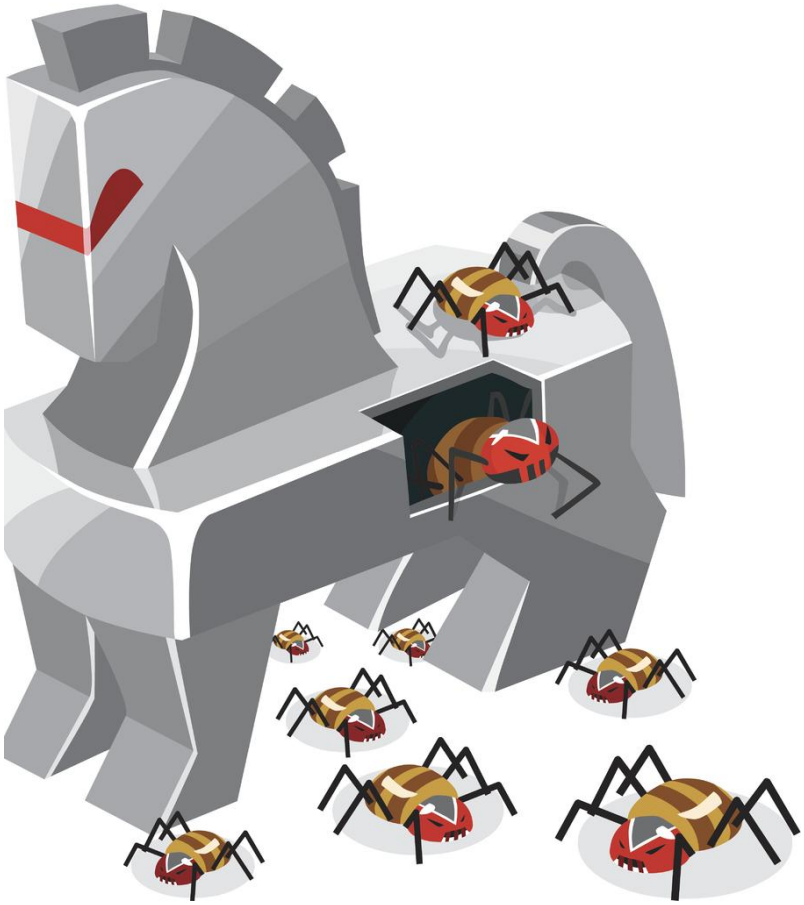
Hardware Trojans in Reconfigurable Computers



project group
SS17+WS17/18

for CS & CE
students

What is a Hardware Trojan?

A computer trojan (trojan horse) is a malicious program used to hack into a computer by misleading users of its true intent.

Software: maliciously inserted code that …

Hardware: maliciously inserted circuit that …

- crashes the computer
- corrupts data
- spies on sensitive information
- implements backdoors
- …

Example: Tiny Banker Trojan, packet sniffing (2015)

Example: Syrian radar failed, rumor about kill switch (2007)

Are Hardware Trojans Really an Issue?

Yes, since there are doubts whether we can trust the chip supply chains!

- explosion of counterfeit chips over the last years

design | manufacturing (typ. offshore) | chip | product

Known threats (rumored and reported incidents)

- kill switches in critical equipment, e.g. fighter jet flight control, radar systems
- key leakage in crypto hardware
- spying on network traffic in routers
- …

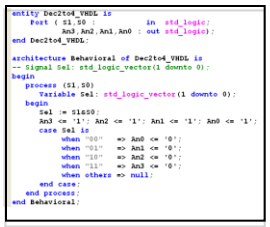
Technology trends create many more possibilities for threats

- misuse of microphones and cameras in Internet-of-Things (IoT) devices
- corporate espionage in Industry 4.0 environments
- personalized health-care
- …

What are Reconfigurable Computers?

Computers that use reconfigurable hardware such as field-programmable gate arrays (FPGAs)

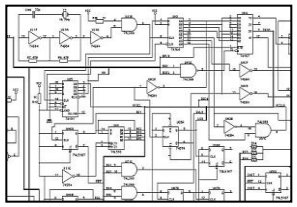
- we can re-program / re-configure the hardware of FPGAs during runtime
- modern FPGAs are huge (millions of gates) and can implement complete systems-on-chip with CPUs, memory, I/O, and hardware accelerators



hardware module
design (IP core)

FPGA tools

FPGA
configuration



design of the
FPGA fabric

manufacturing
(typ. offshore)

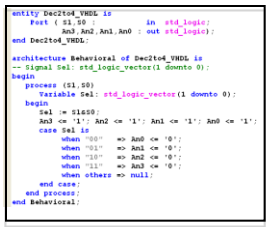
FPGA chip

product

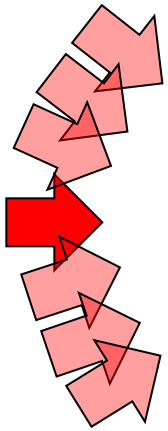
HW Trojans in Reconfigurable Computers?

New type of trojan: trojans in the hardware modules (IP cores)

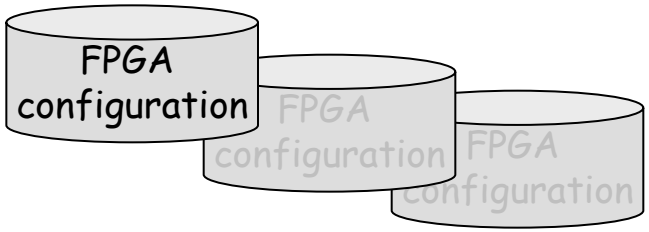
- FPGA configurations include many IP cores from different sources
- the system undergoes many reconfigurations at runtime

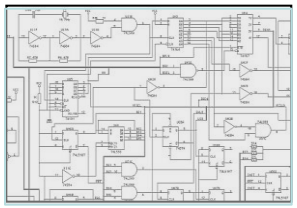


hardware module
design (IP core)



FPGA tools





design of the
FPGA fabric

manufacturing
(typ. offshore)

FPGA chip

product

Project Group ReCoTroy

goals:
1. study and understand hardware trojans in reconfigurable modules
2. develop and demonstrate hardware trojan attacks
3. develop and demonstrate defenses against hardware trojans

develop
first FPGA
AntiSpyWare

demonstration and experimentation environment:
embedded system with Xilinx Zynq programmable platform (SoC)

- dual-core ARM Cortex A9 running Linux
- reconfigurable hardware
- HDMI, audio, 4 x USB 2.0,
  Gigabit Ethernet, PCIe, 500 GB HDD

Project Group ReCoTroy

What you should bring with you

- interest in embedded system design (hardware and/or software)
- interest in security topics
- first experience with programming embedded processors (C/C++, compilers) and/or FPGAs (VHDL, design tools) is very helpful

What you will gain

- knowledge about architectures and tools for embedded systems-on-chip
- practical experience in embedded system design
- expertise in the emerging field of hardware trojans

optional: accompanying course in WS17/18 "Reconfigurable Computing"

Questions?

Today after the presentations ...

or contact supervisors ...

Marco Platzner platzner@upb.de

Tobias Wiersema tobias.wiersema@uni-paderborn.de

or stop by at the ReCoTroy consultation hours

Feb 20, 2017, 1 pm – 3 pm, room O3.113

https://cs.uni-paderborn.de/ceg/teaching/courses/ss-2017/pg-recotroy/