Border Patrol: Improving Hardware Security through Type-Aware Systems Design

Wim Vanderbauwhede
Senior Lecturer/ University of Glasgow School of Computing Science

BORDER PATROL
always on guard

Cambridge, UK
September 11-13, 2017

The Problem

- There are increasing concerns about the safety and security of critical infrastructure such as nuclear power plants, the electricity grid and other utilities, as well as the growing number of IoT devices, in the face of possible cyber attacks.
- As ageing controllers are replaced by smart devices based on Field-Programmable Gate Arrays and embedded microprocessors, the safety of such devices raises many concerns.
- In particular, there are the very real risks of network-based attacks as well as malicious functionality hidden in the silicon or in software binaries, dormant and waiting to be activated.
- Current hardware and software systems are of such complexity that it is impossible to test all parts of the systems to discover such code.

The Impact

- The use of of our approach will dramatically increased safety and security of smart devices and enable novel product developments
- These outcomes will have impact on both society and economy, by helping to safeguard both critical infrastructure and home appliances from cyber attacks.
- Why should you care?
  - Academic Research: Innovations in type theory, programming language design and compilation for HW and SW in Systems-on-Chip
  - Industrial Research: Novel approach to SoC design: safer, more secure, more productive
  - User of the Solution: Guarantees of safety and security and adherence to specifications

Overview of the approach

- Our key idea is to use type systems to encode the formal interface specification of all components in a SoC design
- In other words, the type declarations are the contracts. If the implementation does not follow the contract, the design will not compile.
- For third-party IP cores, the contract can't be verified at design time (the provider of the IP core could lie).
- Therefore we implement run-time type checking on any communication issuing from such blocks
- Hence "Border Patrol"

Overview of the approach

- Our type systems will be able to check many properties:
  - Interface ports and communication protocols
  - Value ranges on communicated information
  - Time derivatives and integration of signals
- The key components of our type system are
  - multi-party session types
  - dependent types
  - subtyping
  - hybrid typing
- We will create a prototype on a Zynq FPGA-based MPSoC system
- Our partners EDF, ABB and Xilinx will provide us with use cases, threat scenarios and specification details.